Secure and guarantee QoS in a video sequence: a new approach based on TLS protocol to secure data and RTP to ensure real-time exchanges.

¹HAMZA TOUIL, ^{1,2}NABIL EL AKKAD, ¹KHALID SATORI ¹LISAC, Faculty of Sciences, Dhar-Mahraz (FSDM), Sidi Mohamed Ben Abdellah University, Fez, MOROCCO

²Laboratory of Engineering, Systems and Applications (LISA), National School of Applied Sciences (ENSA), Sidi Mohamed Ben Abdellah University, Fez, MOROCCO

Abstract: The continued development of networks has significantly contributed to increasing the quantity of information available to replace old intelligence-gathering methods faster and more efficiently. For this, it is necessary to implement services that meet the consumers' requirements and measure precisely the factors that can generate obstacles to any communication, among these causes we can cite strong security and high quality of services. In this work, we implement a secure approach useful in continuous communications in a time axis (video sequence, VOIP call...), the process consists in establishing a well-secured connection between two interlocutors (the server that broadcasts the video sequence and a client) using an AES encryption key of size 256. A step of jitter check (latency variation) periodically is essential for the customer in order to make a decision: If the jitter is within the standards (compared to the tolerable value), we continue to encrypt with the AES256 key, if no, both ends must go through an automatic and uninterrupted fast renegotiation of the video to switch to a small AES key (192,128) to reduce the bandwidth on the channel, this operation must be repeated in an alternative way until the end of the communication.

Keywords: QoS, security, AES, cypher suite, RTP, compromise, Sniffing. DDOS.

Received: October 24, 2020. Accepted: March 15, 2021. Published: March 31, 2021. Published: April 5, 2021.

1. Introduction

Security is a significant challenge in network management and the ever-increasing number of individuals connecting to the Internet. The transmission of sensitive information and the desire to ensure this information's confidentiality has become an essential point in establishing computer networks [1-5]. Therefore, it is crucial to provide a stable technical and legal framework that guarantees adequate data protection. This new trend tends to become more than a rule of competitiveness; it is becoming a genuine legal obligation to protect personal data using adequate and sufficient security measures [8].

The recent strengthening of regulatory requirements has highlighted the security issues of systems (standard, sophisticated, intelligent...), applications, etc. The latter define and implement security policies, sometimes formalized, sometimes empirical, not only to cover the purpose of the system (authentication, prevent unauthorized disclosure of data, prevent unauthorized modification of data, prevent unauthorized use of network or computer resources in general ...). But also, at the level of choice of optimal and efficient algorithms, compatible with other solutions. Furthermore, the quality-of-service strategy specifies several network attributes such as clients or

applications' priority and the actions for processing different traffic categories. However, in our case, we will deal more specifically with the QOS related to multimedia. The process consists of establishing a secured connection between two interlocutors (the server that broadcasts the video sequence and a client) using an AES encryption key of 256. A step of verification of the jitter (latency variation) periodic is essential on the part of the client to make a decision:

If the jitter is within the standards [6,7], the system must keep the encryption with the AES256 key, if not, both ends must go through an automatic and uninterrupted fast renegotiation of the video to switch to a small size AES key (192,128) to reduce the bandwidth on the channel, this operation must be repeated hastily until the end of the communication. This provides a full grasp of the security parameters to be addressed to the QoS objectives. To assess the needs in terms of security and quality of service, the proposed solution allows a compromise was found between better security and a better quality of service. Depending on the different test scenarios, the dimensions of this solution can be evaluated. However, in any case, the requirements are more critical, as they directly impact users [9-14]. In the rest of this document, we will dissect the related works. Then we will simulate the problem that led us to realize this solution and the added value of our work [28].

2. Related Works

A set of studies carried out in this context.[15], Proposed a framework for the quality of protection that corresponds to security and QoS requirements using a multi-attribute decision-making model. In other words, the algorithm puts the encryption keys in order of performance; then if there is degradation at the QOS level, the algorithm replaces the key with another performing month. In [16], Deals with service attacks in telecom networks are widespread and particularly severe. It treats security and QoS in an integrated way using the concept of Quality of Security Service where security is considered a parameter of quality of service. This solution works very well against service attacks.

Some protocols are part of the RTP family, which can ensure a certain level of security. SRTP [17] protocol provides encryption, authentication and integrity of messages and protects against the replay of RTP data. SRTP works in both unicast and multicast mode. In addition to preventing unauthorized eavesdropping on an RTP session, users can also limit the amount of personal information they provide. It recommended that applications do not issue RTCP source description packets without first informing the user. This protocol is robust in terms of security, and this is not the case in QOS, as it performs key changes at a given time interval and does not check the QOS parameters. ZRTP [18] describes a mechanism that allows two communicating parties to exchange encryption keys securely. In order to be able to encrypt traffic using SRTP. Although it is based on using the public key encryption algorithm, it does not require PKI or any particular infrastructure. The dialogue between the two parties carried out using the RTP protocol using specific extensions. Being independent of the signalling protocol is potentially compatible with all VOIP protocols (SIP, H323, Megaco...). A client that does not support ZRTP will ignore these extensions, without impacting communications. The key exchange is done peer to peer and does not require any central server. Infrastructure independence has been a priority in the design of this protocol.

50Qxgtxlgy 'qh'Rt qwqeqn'UUN1VNU0'

The purpose of the protocol is to provide secure data transmission. In this case, asymmetric encryption algorithms are used for authentication (a public-private key pair), and symmetric encryption algorithms (secret key) are used to maintain confidentiality. When a user visits a website, the browser requests certificate information from the server, and the server sends a copy of the SSL certificate together with the public key. Then, the browser checks the certificate, which must match the website's name, the validity date of the certificate, and the presence of a root certificate issued by a trusted certificate authority. If the browser trusts the certificate, it generates a session pre-master secret based on the public key using the highest level of encryption supported by both parties(figure1).



Fig. 1. The steps of SSL communication.

The server decrypts the pre-master secret using its private key, agrees to continue communication, and creates a master secret using encryption. Both parties now use a symmetric key that is only valid for that session. Once completed, the key is destroyed, and the next time you visit the site, the contact process begins again [19,23,24,25].

60S wcrkw{ 'qh'Ugt xkeg0'

Three main actors have essential stakes in designing and provisioning the Internet-based on the Internet Protocol (IP) [20]. These are the sender, the receiver and the Internet Service Provider (ISP). These actors compose the triangle of services (Fig.2). The sender wants to submit any form of traffic at any time (high load, saturation), while the receiver expects to receive all this sent traffic intact, with little delay (short delay, jitter, and packet loss). Also, the third player, the provider, wants to use the minimum possible network capacity per customer (whether sender or receiver) in order to be able to accommodate more customers on its network, resulting in higher profits.



The first objective of QoS is to give priority services, including bandwidth, jitter, and latency. It can also say that QoS represents the set of techniques needed to manage network bandwidth, delay, jitter, and packet loss. Another relevant term that will use shortly is a network flow or stream. A flow can be defined in several ways. One of them refers to a combination of source and destination addresses, source and destination socket numbers, and session identifiers. It can also be defined more broadly as any packet from a particular application or an inbound interface.

Real-Time Protocol (RTP): The first formal effort to support end-to-end, real-time transfer of stream data over network IP. RTP is a session layer protocol, which runs above the Datagram Protocol (UDP) user layer and is therefore transparent to network routers. This is an essential distinction from later technologies and architectures where routers have a key role in providing QoS differentiation. To get a better idea of how a video sequence [21] operating in standards affects traffic flow's bandwidth requirements, we classify them into one primary and two secondary constraints. The primary constraint is that the packet loss rate must be less than 1%. The secondary is that the 95th percentile of the end-to-end delay should be less than 50 ms, and the second constraint that jitter should be less than 30 ms.

70Rquukdkdsdgu'qh'Cvcemu''

This part aims to see the attacks that can cause a blockage on a communication channel such as the sniffing techniques [22] used by malware or hackers to exploit data that passes through a public network. Furthermore, it aims at identifying packets that circulate between communicators. This technique will make it possible to distinguish packets on routers or a communication channel thanks to dedicated tools (Wireshark in our case) connected to a database containing the attack model. If the sniffing system is detected as attacks, the firewall separates the Internet Protocol (IP) address. Then the communication between the attacker's host and the target will be interrupted.

To capture confidential information from the flow of data packets over the network, an attacker must install an appropriate "sniffer" (network protocol analyzer) on the victim's system, e.g., Wireshark, Ettercap, Bettercap, Tcpdump, WinDump. It may not be just software. Sometimes the monitoring is done from a hardware device connected to the system.

DOS/DDOS: Attacks target corporate servers in companies and websites, much less often - individuals' personal computers. The aim of these actions, as a rule, is one: to cause economic damage to those attacked and to remain in the shadows. In some cases, DoS and DDoS attacks are steps in server hacking and are aimed at stealing or destroying information. In fact, a company or website belonging to anyone can become a victim of cybercriminals. Generally, we can distinguish several types: In the case of a massive (volume-based) DDoS attack, many requests are often used, often sent from legitimate IP addresses, so that the site "drowns" in traffic. These attacks aim to "block" all available bandwidth and block legitimate traffic [26]. In a protocol-level attack (such as UDP or ICMP), the goal is to deplete system resources. To do this, open requests are sent, e.g., TCP/IP requests with a fake IP, and due to the exhaustion of network resources, it becomes impossible to process legitimate requests. Typical representatives are DDoS attacks, known in narrow circles as Smurf DDos, Ping of Death, and SYN flood. Another type of DDoS attack at the protocol level involves sending many fragmented packets that the system cannot handle. Layer 7 DDoS attacks are the sending of seemingly harmless requests that appear to result from normal user activity. Botnets and automated tools are generally used to implement them. Notable examples are Slowloris, Apache Killer, Cross-site scripting, SQL-injection, Remote file injection [27].

80Vj g'Rt qr qugf 'Cr r t qc ej ''

The field of intervention of our method is wide; however, we focus on studying the transmission of a video sequence from a server (broadcaster) to a simple client (consumer). The client sends information to the server, such as the SSL protocol version, session ID, and encryption suites, and then the information such as the cryptographic algorithms and keys supported. The server chooses the best encryption suite supported by it and the client, and sends it to the client (Certificate (Public Key, Data)), and then requests the client to send its certificate if necessary. After the client verifies the certificate, it sends the encryption key used to encrypt messages; this is done once and for all in regular communication. However, in our case, we will modify it to be dynamic and automatic and linked to the channel and QoS status. To start with better security, we need to use a more secure key for this, and we need to start the encryption with the AES 256 key. The system will then automatically control the channel status through the existing parameters (latency, jitter...). If abnormal behavior is observed (network saturation, congestion ...), the system must intervene and change the key quickly to a smaller size than the one used initially and then continue the procedure. If stabilization is observed after, the system will change to a large key (figure 4).

6.1 Concept of our method.

The diagram below (Fig.3) describes the steps followed in our method.



Fig. 3. Operating principle of our method.

This Algorithm will allow us to find compromises between various objectives:

> Automate renegotiations: this procedure did not exist before, because the negotiation is done once and for all, at the start of communication, but with this the algorithm we can have renegotiations if necessary, it all depends on the state of the channel, jitter, latency ...

➤ Change the key in an alternative way: this option has two major advantages:

 \checkmark The key used in the session is temporary, and therefore it will be more difficult for a hacker to attack the canal.

 \checkmark There is no need to allocate significant resources to use more keys secure. Alternatively, to implement more or less weak keys to save costs resources. Because thanks to this solution we can make changes between keys in a flexible way.

 \succ Optimization of resources: instead of allocating significant resources to implement solutions in the worst cases, thanks to this algorithm, we can reserve resources compatible with the current situation.

> An equilibrium between security and service quality: i.e., if the channel is loaded, then the latency is important. The algorithm chooses by default the cyphers suites with encryption keys and lightweight hashing to ensure a better quality of service possible.







Our method is set up to satisfy users' needs by minimizing the workload due to the different treatments, i.e., to invent a dynamic algorithm that adapts to the different situations of the channel without any external intervention.

As already evoked the first phase consists of passing by a standard negotiation, the customer sends a hello + the list of cyphers suites that he supports as shown below (figure 5).



Fig. 5. Starting an SSL Negotiation

A modification will be made to the previous phase by applying a filter at the cipher's suits list to support only the AES encryption key and eliminate the DES,3DES keys since they are too much and are not compatible with this kind of exchange. The new list is as illustrated Figure 6.



Fig. 6. Parametric SSL negotiation

If you want to focus on a cipher's components, they usually consist of four parts, as shown in Figure 7.

Protocol Certificat Key Encryptions key Integrity

TLS_RSA_WITH_AES_256_CBC_SHA

Fig. 7. Components of a cipher suits

After the server receives the client request the second filter is going to be applied this time on the server-side to tolerate that the AES key size 256 in the suggestions the goal is to start with a higher security level, using a more secure key of ample size for that we must start the encryption with the key AES_256(we do not take into account the robustness of the hash key in our study)(figure 8).



Fig. 8. Parametric SSL negotiation_ AES256.

The next step is to ensure confidentiality, so the server must send a certificate validated by a CA (Certification Authority))(figure 9).



Fig. 9. Final round of negotiations

After the certificate verification phase on the part of the client, it sends the encryption key used to encrypt the messages; this phase is carried out once and for all in regular communication. However, in our case, we will modify it so that it is dynamic and automatic is linked to the channel and the QoS state. The certificate's sending on the client-side remains optional so that the two interlocutors can securely exchange data.

At this point, we have managed to provide favorable security but assuming we are facing a DDOS attack?

Our method can detect this attack on our flag for the security measures, which can make our task more manageable. The "timestamp" field is available on the RTP frames for our service at the calculation level to the latency variation (JITTER). We remind you that the tolerable value for videos estimated at 40ms.

After every 4 seconds, a check of the different QOS parameters (packet loss, latency, jitter) is done automatically if the system detects one or more abnormal things (e.g., jitter exceeds the tolerable threshold of 40 ms as a result of a DOS attack), i.e., the channel is well loaded and can cause service degradation. So a switch to another small key is essential to reduce the size of the frames sent.

In time, an axis that does not exceed one second, the client must request a small key through a quick renegotiation with the server. However, this time he must propose the AES128 keys in the list of cipher suites.

In the same way, after every 4 seconds, a jitter calculation is done automatically. If the jitter is above the tolerable threshold, we always keep the same key if we move to the next size to increase the security.

6.2 Experiments

To simulate our method, we have used two virtual machines that use a Linux operating system, and the first machine will be the client and the second a secure broadcast server, which can stream videos on demand in a secure mode. The server uses RTP to transport the data in real-time, and SSL to secure the exchanges. One or more clients can retrieve and manipulate the video remotely using the RTSP protocol. To retrieve a video sequence, the client sends a request to create the channel and initialize the session. At this step, the client and the server make exchanges (Certificate, encryption key, cyphers suites, ...) We used the Wireshark tool to capture different interactions. The client sends to the server information such as SSL protocol version, session id, and cypher suites information such as cryptographer algorithms and supported keys. Then the server selects the cypher suite supported by it and the client. Client and server exchange certificates with each other; each certificate contains a public key plus data specific to the certificate. After the certificate verification phase, the client sends the encryption key used to encrypt messages; this phase is performed once and for all in regular communication. However, in our case, we will modify it to be dynamic and automatic is linked to the channel status and the QoS. A standard IP frame with the essential elements (source and destination address, version, flags, fragments, TTL, total length...) encapsulates the data sent (figure10).

<u>F</u> ile	Edit View Go G	Capture <u>A</u> nalyze <u>S</u> tatis	stics Telephony <u>W</u> irele	ss Iools Help Q Q Q II			
si							
No.	Time	Source	Destination	Protocol Length Info			
Ē	22 118.206270743 24 118.54207403 26 119.402624079 28 119.508075244 30 119.540677060 32 119.625717352 34 119.627210461 36 119.632181005	172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.10.0 172.16.10.0 172.16.10.0 172.16.20.0 172.16.10.0	172.16.20.0 172.16.20.0 172.16.10.0 172.16.10.0 172.16.10.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0 172.16.20.0	TLSV12 285 Client Hello TLSV12 136 Server Hello TLSV12 134 Client Key Exchange TLSV12 141 Client Key Exchange TLSV12 141 Client Key Exchange TLSV12 167 Encrypted Handshake Message TLSv12 168 Application Data TLSv12 183 Application Data			

As marked in red, in the preceding figure the number (1) the components of the hello-client frame, (2) the server response, (3) the session encryption, and then (4) the data exchanges.

2) The customer must send that the ciphers-suites whose encryption key is AES256 (as described in Figure 11):

551									
-	1	Time	Source	e	Dest	tination	Protoco	Length Info	
	22	118.20627074	3 172.	6.20.0	172	.16.10.0	TLSv1.	265 Client Hello	
	24	118.54207403	4 172.	16.10.0	172	.16.20.0	TLSV1.	1370 Server Hello, Certificate, Server Key Exchange, Server Hello	Done
	26	119.40262407	9 172.	16.20.0	172	.16.10.0	TLSV1.	141 Client Key Exchange	
	28	119.50807524	4 1/2.	16.20.0	1/2	.16.10.0	ILSV1.	72 Change Cipner Spec	
	30	119.5406//00	0 1/2.	16.29.0	1/2	.16.10.0	ILSV1.	167 Encrypted Handshake Message	
	32	119.025/1/35	2 1/2.	10.10.0	1/2	.10.20.0	TLSV1.	72 Change Cipher Spec	
	34	119.02/21840	1 1/2.	10.10.0	1/2	10.20.0	ILSVI.	167 Encrypted Handshake Message	
	30	119.03002030	5 472	10.20.0	172	10.10.0	TLSV1.	203 Application Data	
	30	119.03218186	0 1/2.	10.10.0	1/2	.10.20.0	ILSV1.	183 Application Data	
		Version: 1	LS 1.2	(0x0303)					
		Random							
		Session II	Lengt	n: 0					
		Linner Su	105 10	00TD 5H					
		and the second second		Married Woman					
	F	 Cipher Sut 	tes (2	5 suites)					
		 Cipher Sul Cipher 	tes (2 Suite:	5 suites) TLS_ECDH	_ECDSA_WITH	H_AES_256_	CBC_SHA384 (0x	(24)	
		 Cipher Sul Cipher Cipher 	tes (2 Suite: Suite:	5 suites) TLS_ECDH TLS_ECDH	_ECDSA_WITH _RSA_WITH_/	H_AES_256_1 AES_256_CB	CBC_SHA384 (0x C_SHA384 (0xc0	24)	
		 Cipher Sul Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite:	5 suites) TLS_ECDHE TLS_ECDHE TLS_RSA_V	_ECDSA_WITH _RSA_WITH_/ ITH_AES_256	H_AES_256_0 AES_256_CBI 6_CBC_SHA2	CBC_SHA384 (0x C_SHA384 (0xc0 56 (0x003d)	24)))	
		Cipher Sul Cipher Cipher Cipher Cipher	tes (2 Suite: Suite: Suite: Suite:	5 SUITES) TLS_ECDHE TLS_ECDHE TLS_RSA_V TLS_ECDH	_ECDSA_WITH _RSA_WITH_/ ITH_AES_256 ECDSA_WITH	H_AES_256_CB AES_256_CB 6_CBC_SHA29 AES_256_CC	CBC_SHA384 (0x C_SHA384 (0xc0 56 (0x003d) BC_SHA384 (0xc1	224) 1) 76)	
		 Cipher Sui Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite:	TLS_ECDH TLS_ECDH TLS_ECDH TLS_RSA_V TLS_ECDH TLS_ECDH TLS_ECDH	_ECDSA_WITH RSA_WITH / ITH_AES_256 ECDSA_WITH RSA_WITH_AE	H_AES_256_CB AES_256_CB 6_CBC_SHA2 AES_256_CB ES_256_CBC	CBC_SHA384 (0x C_SHA384 (0xc0 56 (0x003d) 3C_SHA384 (0xc02 SHA384 (0xc02	(24) () (6)	
		 Cipher Suit Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite:	Suites) TLS_ECDHE TLS_ECDHE TLS_ECDHE TLS_ECDH TLS_ECDH TLS_ECDH TLS_DHE_E	_ECDSA_WITH _RSA_WITH_/ ITH_AES_250 ECDSA_WITH_AE SA_WITH_AE SA_WITH_AE	H AES_256_0 AES_256_0 6_0BC_SHA2 AES_256_0 ES_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_0 8_256_00000000000000000000000000000000000	CBC_SHA384 (0xc0 SHA384 (0xc0 56 (0x003d) 3C_SHA384 (0xc02 _SHA384 (0xc02 SHA386 (0x002 SHA256 (0x0005	224))66)	
		 Cipher Sui Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	Suites) TLS_ECDHE TLS_ECDHE TLS_RSA_I TLS_ECDH TLS_ECDH TLS_DHE_I TLS_DHE_I	ECDSA_WITH RSA_WITH_J ITH_AES_250 ECDSA_WITH_AES SA_WITH_AES SA_WITH_AES SS_WITH_AES SS_WITH_AES	H_AES_256_1 AES_256_CBI 6_CBC_SHA2! AES_256_CBC S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_	CBC_SHA384 (0xc0 C_SHA384 (0xc0) 56 (0x003d) 3C_SHA384 (0xc02) SHA384 (0xc02) SHA386 (0x006b SHA256 (0x006b SHA256 (0x006b	224))) 66)	
		 Cipher Sut Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	Suites) TLS_ECDHE TLS_ECDHE TLS_RSA_V TLS_ECDH TLS_ECDH TLS_DHE_E TLS_DHE_E TLS_DHE_E	ECDSA_WITH RSA_WITH_/ ITH_AES_250 ECDSA_WITH_ RSA_WITH_AES SA_WITH_AES SS_WITH_AES ECDSA_WITH_ ECDSA_WITH_	H_AES_256_0 AES_256_CBI 6_CBC_SHA2! AES_256_CBC 8_256_CBC_5 256_CBC_5 256_CBC_5 256_CBC_5 4_AES_256_CBC_5	CBC_SHA384 (0x C_SHA384 (0xc0 56 (0x003d) 30_SHA384 (0xc02 SHA384 (0xc02 SHA384 (0x006b SHA256 (0x006b SHA256 (0x006b SHA256 (0x006b CBC_SHA (0xc000)	224))) 266)	
		 Cipher Sui Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	Suites) TLS_ECDHE TLS_ECDHE TLS_ECDH TLS_ECDH TLS_ECDH TLS_DHE_I TLS_DHE_I TLS_ECDHE TLS_ECDHE	ECDSA_WITH RSA_WITH_/ ITH_AES_250 ECDSA_WITH_ RSA_WITH_AES SA_WITH_AES SA_WITH_AES _ECDSA_WITH_ _RSA_WITH_AES	H_AES_256_0 AES_256_CB AES_256_CB AES_256_CBC S_256_CBC S_256_CBC S_256_CBC S_256_CBC H_AES_256_0 AES_256_CB AES_256_CB	CBC_SHA384 (0x: C_SHA384 (0x:08 C_SHA384 (0x:09 3C_SHA384 (0x:09 SHA384 (0x:09 SHA384 (0x:09 SHA256 (0x:096 SHA256 (0x:096 SHA256 (0x:096 SHA (0x:0914)	224))) 66)	
		 Cipher Su: Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	5 suites) TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_DHE_I TLS_DHE_I TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA_WITH RSA_WITH J ITH AES_25I ECDSA_WITH_AES SA_WITH_AES SS_WITH_AES ECDSA_WITH_ RSA_WITH_J ITH_AES_250 ITH_AES_250 ITH_AES_250	H_AES_256_0 AES_256_CBI 6_CBC_SHA2! AES_256_CBC S_256_CBC_S S_256_CBC_S S_256_CBC_S H_AES_256_CBI AES_256_CBI AES_256_CBI 6_CBC_SHA	CBC_SHA384 (0xc SHA384 (0xc0 56 (0x003d) 3C_SHA384 (0xc0 SHA384 (0xc0 SHA384 (0xc08 SHA256 (0x006a CBC_SHA (0xc08 CSCA (0xc014) (0x0055) SCA (0x0055) SCA (0x055) SCA (0x05	224))) 26)	
		 Cipher Su: Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	5 SUITES) TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_DHE_I TLS_DHE_I TLS_ECDHI TLS_ECDHI TLS_ECDHI TLS_ECDHI	ECDSA_WITH RSA_WITH_J ITH_AES_256 ECDSA_WITH_AES SA_WITH_AES SS_WITH_AES SS_WITH_AES ECDSA_WITH_ RSA_WITH_J ITH_AES_256 ECDSA_WITH_AES ECDSA_WITH_J ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 ITH_AES_256 I	H_AES_256_1 AES_256_CBI 6_CBC_SHA2: AES_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ H_AES_256_CBI 6_CBC_SHA AES_256_CBI 6_CBC_SHA	CBC_SHA384 (0x C_SHA384 (0xcB 56 (0x083d) 3C_SHA384 (0xc2 SHA384 (0xc2 SHA384 (0xc2 SHA384 (0xc06 SHA356 (0x086a CBC_SHA (0xc064) (0x0805) 3C_SHA (0xc064) (0x0805) 3C_SHA (0xc064)	224) () (6)	
		 Cipher Su: Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	5 SUITES) TLS_ECDH TLS_ECDH TLS_RSA_I TLS_ECDH TLS_ECDH_I TLS_DHE_I TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA_WITH RSA_WITH_J ITH_AES_256 ECDSA_WITH_AES SA_WITH_AES SS_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDSA_WITH ECDS	H AES_256_CB AES_256_CB 6_CBC_SHA2: AES_256_CBC S_256_CBC_S 256_CBC_S H AES_256_CB AES_256_CB 6_CBC_SHA AES_256_CCB 5_56_CBC_SHA AES_256_CBC 5_56_CBC	CBC_SHA384 (0x C_SHA384 (0xc0 G6 (0x003d) 3C_SHA384 (0xc0 SHA384 (0xc0 SHA384 (0xc0 SHA256 (0x006a SHA256 (0x006a SHA (0xc004) (0x004) 3C_SHA (0xc005 SHA (0xc005 SHA (0xc007)	224))) (6)	
		 Cipher Su: Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	5 SUITES) TLS_ECDH TLS_ECDH TLS_RSA_I TLS_ECDH TLS_ECDH_ TLS_DHE_I TLS_DHE_I TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA WITH RSA WITH A TTH AES 250 ECDSA WITH A SSA WITH AES SSA WITH AES ECDSA WITH AES ECDSA WITH AES ECDSA WITH RSA WITH AES SSA WITH AES SSA WITH AES	H AES 256 (HES 256 CBC 5 CBC SHA2: AES 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC H AES 256 CB 6 CBC SHA AES 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC	CBC_SHA384 (0x) _ SHA384 (0x) G (0x)0030 SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA256 (0x) SHA (0x) S	224) () (6)	
		 Cipher Sui Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA_WITH RSA_WITH_A ITH_AES_25/ ECDSA_WITH_AES_25/ ECDSA_WITH_AES SS_WITH_AES ECDSA_WITH_ RSA_WITH_AES_25/ ECDSA_WITH_RSA_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES	H AES 256 CB AES 256 CB 5 CBC SHA2 AES 256 CB S 256 CBC S 256 CBC S 256 CBC S 256 CBC AES 256 CB CBC SHA AES 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC	CBC_SHA384 (0xc) _SHA384 (0xc0 SHA384 (0xc0) SHA384 (0xc0) SHA384 (0xc0) SHA384 (0xc0) CSHA (0xc006) CSHA (0xc006) SHA (0xc007) SHA (0xc07) SHA (0xc07	(24) () (6)	
		 Cipher Sui Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher 	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	SUITES) TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_DHE_I TLS_DHE_I TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON	ECDSA_WITH RSA_WITH_/ ITH_AES_25/ ECDSA_WITH_AES SA_WITH_AES SA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES SA_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_SS_WITH_SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_WITH_SS_W	H AES 256 0 AES 256 CB 5 CBC SHA2 AES 256 CC S 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC 5 256 CBC 6 CBC SHA AES 256 CB 5 256 CBC 5 256 CBC	CBC_SHA384 (0x) SHA384 (0x) SG (0x003d) SC_SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA256 (0x0065 CBC_SHA (0x) SHA (0x0014) (0x0035) SHA (0x0039) SHA (0x0039) SHA (0x0039) SHA (0x0031) SHA (0x0031) SH	224))) (6) (22)	
		 Cipher Suz Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	SUITES) TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_DHE_T TLS_DHE_T TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA_WITH RSA_WITH_/ ECDSA_WITH_/ ECDSA_WITH RSA_WITH_AES SS_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES SS_WITH_AES ECDSA_WITH_AES SS_WITH_AES SS_WITH_AES ECDSA_WITH_AES SS_WITH_AES ECDSA_WITH_AES SS_WITH_AES ECDSA_WITH_AES SS_WITH_AES ECDSA_WITH_AES SS_WITH_AES ECDSA_WITH_AES SS_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH_AES ECDSA_WITH ECDSA_WI	H_AES_256_ AES_256_CB _CBC_SHA2: AES_256_CBC _S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC	CBC_SHA384 (0xc) SHA384 (0xc) 6 (0x003d) 3C_SHA384 (0xc) SHA384 (0xc) SHA256 (0x006a SHA256 (0x006a SHA256 (0x006a SHA256 (0x006a SHA (0xc007) SHA (0xc007) SHA (0xc007) SHA (0x0038) SHA	224))) (6)) (2c)))	
		 Cipher Suz Cipher Cipher Cipher Cipher Cipher Cipher	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	5 SUITES) TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA_WITH RSA_WITH_AUTH_AUTH_AUTH_AUSA_250 ECDSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_250 ECDSA_WITH_ECDSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_VITH_AUSA_VITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITH_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITM_AUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUSA_WITMAUS	H_AES_256_CB AES_256_CBC AES_256_CBC AES_256_CBC S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ AES_256_CCB_ AES_256_GC_ S_6_CBC_SHA3 AES_256_GC_ S_6_CBC_SHA33	CBC_SHA384 (9xc CSHA384 (9xcB CSHA384 (9xcB CSHA384 (9xcB SHA394 (9xcB SHA394 (9xcB SHA394 (9xcB CSHA (9xcB05) SHA (9xcB05) SHA (9xcB05) SHA (9xcB05) SHA (9xcB03) SHA (9xcB	224))66) 22e)	
		 Cipher Suz Cipher Cipher Cipher Ci	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA_WITH RSA_WITH_A ECDSA_WITH_RSA_WITH_A SA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITH_ASSA_WITASAAASAAASAAAAASAAAAAAAAAAAAAAAAAAAAA	H_AES_256_CB AES_256_CBC S_CBC_SHA2: AES_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ AES_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_CBC_ S_256_GM_SHA33 AES_256_G S_256_GM_SHA33	ERC SHA384 (bxc) SHA384 (bxc) SHA384 (bxc) SHA384 (bxc) SHA384 (bxc) SHA384 (bxc) SHA384 (bxc) SHA256 (bxc) SHA256 (bxc) SHA (bxc) SHA384 (bxc) SHA	724))) 66) (72c))) Ye)	
		 Cipher Suz Cipher Cipher Cipher Ci	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite:	Suites) TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH	ECDSA_WITH RSA_WITH_AI COSA_WITH_AI RSA_WITH_AI RSA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI ECDSA_WITH RSA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_AI SA_WITH_SA_WITH_AI SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_WITH_SA_W	H AES 256 CB AES 256 CB CBC SHA22 AES 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC AES 256 CB CBC SHA AES 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC AES 256 CBC S 256 C	CEC_SHA384 (0xC SHA384 (0xC 56 (0x0830) 3C_SHA384 (0xC SHA384 (0xC SHA384 (0xC SHA384 (0xC SHA384 (0xC SHA (0xC SHA) (0xC SHA (0xC SHA384 (0xC) SHA384 (0xC SHA384 (0xC) SHA384 (0xC) SH	224))) (6)) (2c))) (2c))) (2c)	
		 Cipher Suz Cipher Cipher Cipher Cipher Cipher Cipher	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	5 SUITES) TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH TLS_ECDH	ECDSA WITH RSA_WITH A ECDSA_WITH A ECDSA_WITH RSA_WITH A SA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH RSA_WITH A ECDSA_WITH A ECDSA	H_AES_256_CB AES_256_CBC AES_256_CBC AES_256_CBC S_256_CBC S_256_CBC S_256_CBC S_256_CBC AES_256_CBC AES_256_CBC S_256_CBC S_256_CBC S_256_CBC S_256_CBC S_256_CBC S_256_CBC S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_256_CCB S_2	LBC_SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA (0x) SHA384 (0x) SHA38	224)) 66) (22c))) 10 10 10 10 10 10 10 10 10 10	
		 Cipher Suz Cipher Cipher Cipher Ci	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	Sultes) TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_DHE_I TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH TLS_ECOH	ECDSA WITH RSA_WITH_A ECDSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITH_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_WITA_RSA_	H AES 256 (B AES 256 (CB) 5 (CC) SH225 (CB) 5 (CC) SH225 (CB) 5 (CC) SH25 (CB) 5 (CC) SH25 (CB) 5 (CC) SH25 (CB) 5 (CB) SH2 (CB) 5 (CB) SH2 (CB) 5 (CB) SH2 5 (CB) S	CBC SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA384 (0x) SHA256 (0x)086a SHA256 (0x)086a SHA (0x)014 (0x)014 SHA (0x)014 SHA (0x)014 SHA (0x)014 SHA (0x)014 SHA (0x)014 SHA34 (0x) SHA34 (224))) (6)) (2c))))))	
		 Cipher Suz Cipher Cipher Cipher Cipher Cipher Cipher Cipher Cipher<!--</td--><td>tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su</td><td>TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_EC</td><td>ECDSA WITH A RSA_WITH A ECDSA_WITH, RSA_WITH, AES SS_WITH, AES SS_WITH, AES SS_WITH, AES ECDSA_WITH, RSA_WITH, AES SS_WITH, AES SS_WITH, AES COSA_WITH, RSA_WITH, ATH, ASA_WITH, AES SS_WITH, AES SS_</td><td>H AES 256 CB AES 256 CB AES 256 CB S 256 CB S 256 CB S 256 CBC S 256 CBC S 256 CBC H AES 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC AES 256 CBC AES 256 CBC S 256</td><td>LBC SHA384 (0x) 2 SHA384 (0x) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0835) 5 (9x164) 5 (9x0835) 5 (9x164) 5 (</td><td>224))66) 1222))1 129)</td><td></td>	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_ECONH TLS_EC	ECDSA WITH A RSA_WITH A ECDSA_WITH, RSA_WITH, AES SS_WITH, AES SS_WITH, AES SS_WITH, AES ECDSA_WITH, RSA_WITH, AES SS_WITH, AES SS_WITH, AES COSA_WITH, RSA_WITH, ATH, ASA_WITH, AES SS_WITH, AES SS_	H AES 256 CB AES 256 CB AES 256 CB S 256 CB S 256 CB S 256 CBC S 256 CBC S 256 CBC H AES 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC S 256 CBC AES 256 CBC AES 256 CBC S 256	LBC SHA384 (0x) 2 SHA384 (0x) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0834) 5 (9x0835) 5 (9x164) 5 (9x0835) 5 (9x164) 5 (224))66) 1222))1 129)	
		 Cipher Suz Cipher Cipher Cipher Ci	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_ECONE TLS_EC	ECDSA, WITH RSA, WITH, RSA, WITH, RSA, WITH, RSA, WITH, ASS SS, WITH, SS, WITH, ASS SS, WITH, SS, WITH, S	H AES 256 0 BES 256 0 BES 256 0 S 256 0 S 256 0 S 256 0 S 256 0 S 256 0 AES 256 0 AES 256 0 AES 256 0 S 256 0	CBC_SHA384 (0x) SHA384 (0x) SHA15 (0x) SHA16 (0x) SHA16 (0x) SHA (0x) <	224))) (6)) (2c))) (2c))) (2c)	
		 Cipher Suz Cipher Cipher Cipher Ci	tes (2 Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Suite: Su	TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_DHE_I TLS_DHE_I TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_ECON TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS_DHE_I TLS	ECDSA, MITH ESA, MITH, J ITH, AES, 250 ECDSA, WITH, AES SS, WITH, AES SS, WITH, AES SS, WITH, AES ECDSA, WITH, AES SS, WITH, AES SM,	H AES 256 (A AES 256 (CB ES 256 (CB S 256 (CB) S 256 (CB S 256 (CB) S 256 (CB S 256 (CB) S 256 (CB)	280 SHA384 (bw SHA384 (bw SHA384 (bwc) SHA384 (bwc) SHA384 (bwc) SHA384 (bwc) SHA384 (bwc) SHA256 (bwo) SHA (bwc) SHA (bwc)	224))66) 1 (22c))) 190)	

Fig.11. The list of AES_256 suite ciphers provided by TLS1.2.

3) The server chooses the first support cipher on its part, as shown below with the number (2) in red (Figure 12).

Ŧ	Ethernet II, Src: Vmware_e3:c9:d5 (00:0c:29:e3:c9:d5), Dst: Vmware_4a:35:40 (00:0c:29:4a:35:40)
	Destination: Vmware_4a:35:40 (00:0c:29:4a:35:40)
	Source: Vmware_e3:c9:d5 (00:0c:29:e3:c9:d5)
	Type: IPv4 (0x0800)
÷	Internet Protocol Version 4, Src: 172.16.20.0, Dst: 172.16.10.0
	0100 = Version: 4
	0101 = Header Length: 20 bytes
	Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
	Total Length: 251
	Identification: 0xbacd (47821)
	Elags: 0x02 (Don't Fragment)
	Frament offset: 0
	Time to live: 64
	Protocol: TCP (6)
	Needer checksum: 0x000f [validation disabled]
	Source: 172 16 20 0
	Dour te. 172.10.20.0
	Contraction: 1/2.10.10.0
	[Source GeolP: Unknown]
	[Destination GeolP: Unknown]
	Iransmission Control Protocol, Src Port: 42566 (42566), Dst Port: 443 (443), Seq: 1, ACK: 1, Len: 199
	Secure Sockets Layer
Θ	000 00 0c 29 4a 35 40 00 0c 29 e3 c9 d5 08 00 45 00)J5(0)E.
Θ	910 80 fb ba cd 40 80 40 86 89 8f ac 10 14 88 ac 18().().()
Θ	929 0a 00 a6 46 01 bb de 6a a3 7a ce b4 a3 69 80 18 Fj .zi
Θ	330 00 e5 4b f8 00 00 01 01 08 0a 00 03 06 bf 00 02K
Θ	940 9d 1d 16 03 03 00 c2 01 00 00 be 03 03 59 87 4b
Θ	950 f1 da 2b 93 52 ee 15 5f 12 bd bd 81 46 8b 24 65+.RF.\$e
Θ	360 29 ff f5 83 93 dd 1f 55 34 5a d1 17 bb 00 00 32)Ū 4Z2
Θ	970 c0 24 c0 28 60 3d c0 26 c0 2a 60 6b 60 6a c0 0a (\$,(.=.& .*.k.1

Fig. 10. Initialization of the SSL session under Wireshark.

A				
A.,		4 🖛 🖷 1		
5	1			
0.	Time Source	Destination	Protocol I	ength Info
	22 118.206270743 172.16.20.0	172.16.10.0	TLSv1.2	265 Client Hello
	24 118.542074034 172.16.10.0	172.16.20.0	TLSv1.2	1370 Server Hello, Certificate, Se
	26 119.402624079 172.16.20.0	172.16.10.0	TLSv1.2	141 Client Key Exchange
	28 119.508075244 172.16.20.0	172.16.10.0	TLSv1.2	72 Change Cipher Spec
	30 119.540677060 172.16.20.0	172.16.10.0	TLSV1.2	167 Encrypted Handshake Message
	32 119.025/1/352 1/2.10.10.0	172.10.20.0	TLSV1.2	12 Change Cipner Spec
	26 110 620020500 172 16 20 0	172 16 10 0	TLSV1.2	262 Application Data
	38 119 632181005 172 16 10 0	172 16 20 0	TLSV1.2	183 Application Data
T	apertication Control Protocol Src B	2.10.10.0, 051. 1/2.1	0.20.0	
Se	 analisatis Layer Curre Sockets Layer: Handshake P Content Type: Handshake (22) Version: TLS 1.2 (0x0393) Length: 1299 Handshake Type: Server Hell Length: 77 Version: TLS 1.2 (0x0393) 	Yort: 443 (443), Dst F rotocol: Multiple Han lo ⊃ (2)	ort: 42566 (42	2566), Seq: 1, Ack: 200, Len: 1304 s
Se	 Sockets Layer Folded, 34 C for the sockets Layer TLSV12. Record Layer: Handshake (22) Version: TLS 1.2 (0x0303) Length: 1299 Handshake Protocol: Server Hell Length: 77 Version: TLS 1.2 (0x0303) Random Session ID: 50724445557744555774455577445557744555774544555774544555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557744555774455577445557574455575745555757457575757575757575757575757757	ort: 443 (443), Dst F rotocol: Multiple Han Lo > (2)	ort: 42566 (42 dshake Message 4ab45c790dd5	566), Seq: 1, Ack: 200, Len: 1304 s
Se	 analisatis Soli Control Protocol, site P curre Sockets Layer: Handshake P Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 1299 Handshake Type: Server Hell Langth: 77 Version: TLS 1.2 (0x0303) Random Session ID Length: 32 Session ID Length: 32 Session ID: SCOME, SAN Compression Method: null (9) Extensions Length: 5 	ort: 443 (443), Dst F rotocol: Multiple Han 10 0 (2) WITH <u>AES_256_CBC_SHA</u>	ort: 42566 (42 dshake Message 4 ab15c700dd5 384 (Øxc028)	2566), Seq: 1, Ack: 200, Len: 1304 s
56	<pre>anare Sockets Layer TLSv12. Record Layer: Handshake (22) Version: TLS 1.2 (9x393) Length: 1299 Handshake Protocol: Server Hell Length: 1299 Wandshake Protocol: Server Hell Length: 77 Version: TLS 1.2 (9x393) Random Session ID: Defath: 32 Session ID: Length: 32 Session ID: Length: 32 Session ID: Softwitzsorreed Cipher Suite: TLS COME_RSA Compression: renegotiation_inf Per : renegotiation_info Length: 1 Famegotiation Info extension</pre>	ort: 443 (443), Dst F rotocol: Multiple Han 10 0 (2) WITH <u>AES_256_CBC_SHA</u> 70 (0stf01) 100	ort: 42566 (42 dshake Message 4ab f5c790dd5 384 (0xc028) ;	2566), Seq: 1, Ack: 200, Len: 1304 s
Se	 Sockit S Layer Sockit S Layer TLSV1.2 Record Layer: Handshake (22) Version: TLS 1.2 (9x393) Length: 1299 Handshake Protocol: Server Hellc Length: 1299 Handshake Protocol: Server Hellc Length: 77 Version: TLS 1.2 (9x393) Random Session ID: Softwice Server Hellc Cipher Source: TLS ECOHE, RSA Cipher Source: InS. ECOHE, RSA Cipher Source: renegotiation_inf Type: renegotiation_info Length: 1 Rengotiation Info extens Handshake Protocol: Certificate Handshake Protocol: Certificate Length: 877 Certificates Length: 874 	ort: 443 (443), Dst F rotocol: Multiple Han (0 (2) WTH AES 256 CBC SHA (0 (ff01) ion (11)	fort: 42566 (42 dshake Message 4abf5e790dd5 884 (0xc028)	2566), Seq: 1, Ack: 200, Len: 1304 s
Se	 Alama Sacht Colligner Holded, Ster Franking, Ster Ster Ster Ster Ster Ster Ster Ster	ort: 443 (443), Dst F rotocol: Multiple Han 0 (2) WITH AES 256 CBC SHA (0xff01) 0 (11)	fort: 42566 (42 dshake Message 4ab f5c798dd5 384 (0xc028) ;	2566), Seq: 1, Ack: 200, Len: 1304 s
Se	<pre>aure Societ Statu TLSV12 Record Layer: Handshake (22) Version: TLS 1.2 (0x0303) Length: 1299 * Handshake Protocol: Server Hell Length: 1299 * Handshake Protocol: Server Hell Length: 77 Version: TLS 1.2 (0x0303) * Random Session ID: 5074445037466 Cipher Suite: TLS_EOUHE_RSA Compression Record: Holl (0) Extension: renegotiation_inf Type: renegotiation_inf Upe: Trenegotiation_inf Upe: Trenegotiation_inf Settension: renegotiation_inf Length: 1 * Extension: Renegotiation_inf Length: 877 Certificates Length: 874 > Certificates (074 bytes) * Handshake Protocol: Server Key Handshake Protocol: Server Key Length: 329</pre>	ort: 443 (443), Dst F rotocol: Multiple Han lo o (2) MITH <u>AES_256_CBC_SHA</u> Yo (0xff01) ion % (11) Exchange (12)	fort: 42566 (42 dshake Message 4ab f5c790dd5 884 (0xc028)	2566), Seq: 1, Ack: 200, Len: 1304 s

Fig.12. The choice of Cipher suit

4) After starting the video playback, the resulting packets are encrypted using the denial function during the negotiation and write key. The algorithms used for encryption are AES 256(figure 13).

	۹ 🗰 🏟 📓 🕯	5 👱 📃 @, @, @, 🎚
SSI SSI		
o. Time Source	Destination	Protocol Length Info
22 118.206270743 172.16.20.0	172.16.10.0	TLSv1.2 265 Client Hello
24 118.542074034 172.16.10.0	172.16.20.0	TLSv1.2 1370 Server Hello, Certificate, Server Key Exchange, Server Hel
26 119.402624079 172.16.20.0	172.16.10.0	TLSv1.2 141 Client Key Exchange
20 119.0000/0244 172.10.20.0	172.10.10.0	TLSV1.2 72 Change Cipiter Spec
32 110 625717352 172 16 18 9	172 16 20 0	TI Su1 2 72 Channe Cinher Sner
34 119.627210461 172.16.10.0	172.16.20.0	TLSv1.2 167 Encrypted Handshake Message
36 119.630020508 172.16.20.0	172.16.10.0	TLSv1.2 263 Application Data
38 119.632181005 172.16.10.0	172.16.20.0	TLSv1.2 183 Application Data
Frame 38: 183 bytes on wire (1464 b Ethernet II, Src: Vmware_4a:35:40 (Internet Protocol Version 4, Src: 1 Transmission control Protocol, Src Secure Sockets Layer • TLSV.1.2 Record Layer: Application Content Type: Application Data Version: TLS 1.2 (208303)	its), 183 bytes captur 30:0c:29:4a:35:40), Ds 72.16.10.0, Dst: 172.1 Port: 443 (443), Dst P 1 Data Protocol: http (23)	ed (1464 bits) on interface 0 1: Vmaare_e3:09:05 (00:00:20:e3:09:05) 5.20.0 ort: 42566 (42566), Seq: 1412, Ack: 579, Len: 117
Encrypted Application Data: a	19ecb335c3598a114d6478	lb515054af7a5dcc586579182

Fig. 13. Data Encryption.

As already mentioned, the algorithm must work in different scenarios. It must also be able to automate the change of keys; for this, we will discuss both solutions:

Free channel: in ordinary cases using two virtual machines connected, a server and a client, then observe the results under Wireshark.

Saturated channel: in this case, we used the Hping3 tool to apply a DOS attack, to load the channel and see the behavior of the algorithm.

5) Free Channel

After starting the video at the client, the calculation of the different QOS parameters (latency, jitter.) is done automatically every 4 seconds. If one or more parameters exceed the recommended thresholds, the key must be changed. The encryption is carried out with the AES_256 key (Figure 14).



Fig.14. encrypt with the AES256 key

6) Channel saturated

As explained, Denial of Service is a technique that consists of sending a data stream that is too large concerning what the target can receive and process. If someone has an IP address and wants to deny you access to the Internet or block access to your site, they will be able to do so if they have a sufficiently large connection. It will then flood and saturate upload bandwidth, which will cause a massive disruption to Internet Traffic in both directions. After performing a DOS attack with the Hping3 tool to saturate the channel, it turns out that the algorithm only uses the AES_128 key to minimize the packet size and manage network congestion.

The client starts the encryption with the AES_256 key to having a reliable security level. However, as soon as the jitter exceeds the 30ms threshold, it is necessary to automatically change the key to AES_128 to reduce the frames' size and facilitate the communication as mentioned (figure 15).



Fig.15. The exchange of the key to AES_128

90E qpenwkqpu''

This study has allowed us to move on to a more important phase that citing the different needs, dysfunctions, and challenges we have encountered. Afterward, we carried out studies on the requirements and the different possible approaches to realize this hybrid algorithm based on RTP and SSL protocols.

The security provided by standard RTP is insufficient because it does not support authentication, and its default encryption algorithm (DES) is fragile at present and simpler to hack.

The biggest security challenge is the management of security keys, how to distribute them, how to store and update them, how to protect them from hackers. For this purpose, we thought about realizing a dynamic and automatic security solution.

References

- [1] Mohammed A. Al-Maqri, Ali Mohammed Mansoor Aznul Qalid Sabri3 Sri Devi Ravana4 Hussein Soubhi Yaseein; High performing multimedia transmission approach based on QoS support and admission control over IEEE 802.11e networks, International Journal of Communication Systems,march 2020. https://doi.org/10.1002/dac.4193
- [2] Serhrouchni. ;Integration of the digital signature in the protocol SSL/TLS Intégration de la signature numérique au protocole SSL/TLS; Annales des Telecommunications/Annals of Telecommunications, P 522-541,May/June 2006.

- [3] Hu, Fan, Zhang; An effective differential power attack method for advanced encryption standard, P (58-61); International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019.
- [4] Nakasone, T., Li, Y., Yu, S; Key-Dependent Weakness of AES-Based Ciphers under Clockwise Collision Distinguisher; International Conference on Information Security & Cryptology. (2012).
- [5] Douglas_R._Stinson, Maura_B._Paterson;
 Cryptography théorie and pratices ; International Standard Book Number-13: 978-1-1381-9701-5,2019.
- [6] Pisheh, M.A.Z., Sheikhi, A; DETECTION AND COMPENSATION OF IMAGE SEQUENCE JITTER DUE TO AN UNSTABLE CCD CAMERA FOR VIDEO TRACKING OF A MOVING TARGET; Proceedings - 2nd International Symposium on 3D Data Processing, Visualization, and Transmission. Pages 258-261,2004.
- [7] Yang, C.,Ling, Y.,Li, X; Information encryption algorithm in power network communication security model; IOP Conference Series: Materials Science and Engineering, december 2019.
- [8] Kambourakis, G., Rouskas, A., Gritzalis, S. ; Using SSL/TLS in authentication and key agreement procedures of future mobile networks (2002) 2002 4th International Workshop on Mobile and Wireless Communications Network, MWCN 2002, art. no. 1045713, pp. 152-156. doi: 10.1109/MWCN.2002.1045713.
- [9] Acharya, Bibhudendra, et al; Image encryption using advanced hill cipher algorithm. International Journal of Recent Trends in Engineering 1.1 (2009): 663-667.
- [10] Ali Mansouril · Xingyuan Wang1,2 ; Image encryption using shuffled Arnold map and multiple values manipulations; Springer-Verlag GmbH Germany, part of Springer Nature 2020
- [11] Hofmann, G.R; The modelling of images for communication in multimedia environments and the evolution from the image signal to the image document; Vis. Comput. 9(6), 303–317 (1993).
- [12] Lin, C.-H., Chao, M.-W., Liang, C.-Y., Lee, T.-Y; A novel semi-blind-and-semi-reversible robust watermarking scheme for 3D polygonal models; Vis. Comput. 26(6), 1101–1111 (2010).
- [13] Tu, S.-C., Tai, W.-K Isenburg, M., Chang, C.-C; An improved data hiding approach for polygon meshes; Vis. Comput. 26(9), 1177–1181 (2010).
- [14] Li, G., Wang, L ; Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform; Vis. Com- put. 35(9), 1267–1277 (2019).
- [15]Tarik Taleb ; Yassine Hadjadj Aoul ; Abderrahim Benslimane; Integrating Security with QoS in Next Generation Networks 2010 IEEE Global

Telecommunications Conference GLOBECOM 2010, 6-10 Dec. 2010.

- [16] Aiash, Mahdi, Mapp, Glenford E. and Lasebae, Aboubaker; Security and QoS integration for protecting service providers in hterogeneous environments; International Journal of Computer Science, 38 (4). pp. 384-393. ISSN 1819-656X,2011.
- [17] (Bud) Bates, Regis J; Securing VOIP || Other protocols SRTP, ZRTP, and SIPS; 10.1016/B978-0-12-417039-1.00006-1;2015.
- [18] Riccardo Bresciani and Andrew Butterfield; A formal security proof for the ZRTP Protocol; International Conference for Internet Technology and Secured Transactions, ICITST 2009 5402595
- [19] Jonathan_Katz, Yehuda_Lindell; INTRODUCTION TO MODERN CRYPTOGRAPHY Second Edition 500; International Standard Book Number-13: 978-1-4665-7027-6,2015
- [20] Bushra Anjum and Harry Perros ; Bandwidth Allocation for Video under Quality of Service Constraints ; Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc;2015
- [21]Seetha, S., Francis, S.A.J., Kanaga, E.G.M., Daniel, E., Durga, S. A framework for multi-constraint multicast routing in wireless mesh networks. In 2019 Fifth international conference on advanced computing & communication systems (ICACCS) (2019) IEEE, Mar, 2019, pp. 445-451.
- [22] Atoum, Y., Liu, Y., Jourabloo, A., Liu, X. Face antispoofing using patch and depth-based CNNs (2018) IEEE International Joint Conference on Biometrics, IJCB 2017, 2018-January, pp. 319-328.
- [23] F. Elazzaby, N. El Akkad and S. Kabbaj. A new encryption approach based on four squares and Zigzag. The 1st international conference on Embedded Systems and Artificial Intelligence, ESAI (2019).
- [24] M. Es-sabry, N. El akkad, M. Merras, A.Saaidi and K.Satori. A New Color Image Encryption Using Random Numbers Generation And Linear Functions. The 1st international conference on Embedded Systems and Artificial Intelligence, ESAI (2019).
- [25] Y, Qiao, Yu, F. Richard, Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing, IEEE Communications Magazine 53(4), 52-59 (2015).
- [26] R.V. Deshmukh, K.K. Devadkar; Understanding DDoS Attack & Its Effect in Cloud Environment; Procedia Comput. Sci 49(1), 202–210 (2015).
- [27] M. Monika, Y. Singh, A Review; DoS and DDoS Attacks, International Journal of Computer Science and Mobile Computing 4(6), 260-265 (2015)

[28] Hamza TOUIL; Nabil EL AKKAD; Khalid SATORI: Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers: International Conference on Intelligent Systems and Computer Vision (2020).

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0 <u>https://creativecommons.org/licenses/by/4.0/deed.en_US</u>