Network Security within Computer Networking and the TCP/IP Suite

1. Introduction to Network Security and Cryptography in the TCP/IP Suite:
   The proliferation of digital communication in the modern era has made network security an increasingly critical concern. The very nature of network transmissions introduces inherent vulnerabilities, necessitating robust mechanisms to protect sensitive information.1 The Transmission Control Protocol/Internet Protocol (TCP/IP) suite serves as the foundational communication protocol for the vast majority of internet and intranet operations.1 Consequently, a thorough understanding of the security mechanisms integrated within and alongside this protocol suite is paramount for safeguarding digital interactions.
   The TCP/IP model provides a conceptual framework for how data is transmitted across networks. This model is structured into four distinct layers: the Network Access layer, the Internet layer, the Transport layer, and the Application layer.[5] Each layer is responsible for specific functions in the data transmission process, and security mechanisms are implemented at various levels to address different vulnerabilities and provide varying degrees of protection.[7] The flexibility inherent in the TCP/IP architecture, while enabling widespread connectivity, also creates potential avenues for unauthorized interference, underscoring the importance of a strong security focus to ensure data remains protected during transit.[1]
   At the heart of network security lies the field of cryptography. Cryptography can be defined as the science and art of transforming messages to render them secure and resilient to attacks.[13] It provides the essential building blocks for achieving fundamental security services in network communication, including confidentiality, ensuring data privacy; integrity, maintaining data accuracy and preventing unauthorized modification; authentication, verifying the identities of communicating parties; and non-repudiation, preventing a sender from denying their actions.[13] Without the application of cryptographic techniques, data transmitted across networks would be susceptible to easy interception and comprehension by unauthorized entities.
2. Symmetric Key Cryptography:
   Symmetric key cryptography is a fundamental type of encryption that employs a single secret key for both the processes of encrypting and decrypting information.17 This key serves as a shared secret that must be known to all parties involved in the secure communication.26 The encryption process involves transforming the original readable data, known as plaintext, into an unreadable format called ciphertext. This transformation is achieved using an encryption

algorithm in conjunction with the secret key. To reverse this process and retrieve the original plaintext, the recipient uses the same secret key along with a corresponding decryption algorithm.18

Various alternative terms are used to refer to symmetric key cryptography, including secret-key encryption, single-key encryption, shared-key encryption, one-key encryption, and private-key encryption.[29] The efficiency of symmetric encryption algorithms makes this method particularly well-suited for encrypting large volumes of data.[1] This speed advantage arises from the relative simplicity of the mathematical operations involved in symmetric algorithms compared to their asymmetric counterparts.

Within the context of the TCP/IP suite, symmetric key cryptography plays a crucial role in ensuring confidentiality during network communication. Confidentiality is maintained by rendering the data incomprehensible to anyone who does not possess the shared secret key.[18] For instance, in the Transport Layer, protocols such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) utilize symmetric encryption algorithms, such as the Advanced Encryption Standard (AES), to encrypt the data stream exchanged between clients and servers after a secure handshake process has established a shared secret.[1] Similarly, at the Network Layer, Internet Protocol Security (IPsec) employs symmetric encryption to ensure data confidentiality for Virtual Private Network (VPN) connections and other secure network communications.[13] The overall security provided by symmetric encryption is directly dependent on both the strength of the specific encryption algorithm employed and the secrecy of the key itself. Therefore, it is of paramount importance to utilize robust algorithms and to implement stringent measures for managing these secret keys securely.[17] While symmetric encryption is highly effective in ensuring confidentiality, it is important to note that it does not inherently provide mechanisms for authentication, verifying the sender's identity, or non-repudiation, preventing the sender from denying their actions.[17] These additional security services necessitate the implementation of separate cryptographic techniques.

Several common symmetric key algorithms are widely used in networking environments. These include the Data Encryption Standard (DES) and the more modern and secure Advanced Encryption Standard (AES).[1] Symmetric encryption algorithms can be broadly categorized into block ciphers and stream ciphers. Block ciphers, such as AES, encrypt data in fixed-size blocks of bits (for example, 128 bits), whereas stream ciphers, such as RC4, encrypt data one bit or byte at a time.[28] The selection of a particular symmetric encryption algorithm is typically guided by factors such as the specific security level required for the application, the performance characteristics of the algorithm, and its compatibility with the

existing infrastructure.

3. The Data Encryption Standard (DES):
   The Data Encryption Standard (DES) is a symmetric block cipher that was designed to encrypt data in fixed-size blocks of 64 bits, producing corresponding 64-bit blocks of ciphertext.16 DES utilizes a 56-bit key for the encryption process, although it accepts a 64-bit key as input. The additional 8 bits in the 64-bit input key are used for parity checking, a basic form of error detection.47 The core of the DES algorithm consists of 16 iterative rounds, where each round involves a series of substitution and permutation operations performed on the data block.16 The underlying structure of DES is based on the Feistel cipher, a design principle that divides the data block into two halves and processes them through multiple rounds using a subkey derived from the main key.49
   The design of DES, particularly the specific substitution boxes (S-boxes) used within the algorithm, was a subject of considerable debate and controversy during its development. This was partly due to the involvement of the National Security Agency (NSA) and the decision to reduce the key size from the 128 bits used in its predecessor, Lucifer, to 56 bits.[47] The secrecy surrounding the design choices for the S-boxes fueled suspicions among some cryptographers that there might be undisclosed vulnerabilities or "backdoors" intentionally introduced by the NSA. However, subsequent analysis of the DES algorithm suggested that its design was actually quite robust against the cryptanalytic techniques known publicly at the time.
   DES holds significant historical importance in the realm of network security. It was developed by IBM in the early 1970s and was officially adopted as a US federal standard in 1977.[47] This standardization marked a crucial step in recognizing the need for publicly vetted cryptographic algorithms to protect sensitive data. Over the years, DES became a widely implemented symmetric-key block cipher and served as a de facto international standard for ensuring the security of business and commercial data.[49] It found applications in various domains, including securing financial transactions and even in the generation of random numbers.[52] DES was the first publicly available encryption standard created by the US government, which contributed significantly to the advancement of cryptographic practices in the commercial sector.[62]
   Despite its widespread adoption and historical significance, DES suffers from several limitations that ultimately led to its obsolescence as a primary encryption standard. The most significant of these limitations is its relatively short key length of 56 bits.[47] With the rapid advancements in computing power, particularly the increase in processing speeds, this key length became increasingly vulnerable to brute-force attacks. In 1998, the Electronic Frontier Foundation's (EFF) "Deep

Crack" machine successfully demonstrated the feasibility of breaking a DES key in a matter of hours, highlighting the algorithm's insecurity against modern computational capabilities.[52] In addition to its small key size, DES has also been found to be susceptible to cryptanalytic attacks such as differential cryptanalysis and linear cryptanalysis, which can exploit statistical patterns in the ciphertext to potentially recover the key.[48] Furthermore, the 64-bit block size of DES can present challenges when encrypting large volumes of data, as it might require specific modes of operation that could introduce their own security considerations.[29] Compared to newer encryption algorithms like AES, DES is also relatively slow when implemented in software, as it was originally designed with hardware implementation in mind.[53] Recognizing these limitations, the National Institute of Standards and Technology (NIST) officially withdrew DES as a federal standard in 2005 and recommended the adoption of the Advanced Encryption Standard (AES) as its successor.[52] While Triple DES (3DES) was used as an interim solution to increase the key size, it too is now being phased out in favor of more efficient and secure algorithms like AES.[29] The short key length of DES was the primary factor that rendered it vulnerable to modern computing capabilities and ultimately led to its replacement by stronger encryption standards.[47]

4. The Advanced Encryption Standard (AES):
   The Advanced Encryption Standard (AES) is a highly secure symmetric block cipher that has become the prevalent encryption algorithm worldwide.74 AES operates on a fixed block size of 128 bits, which is equivalent to 16 bytes of data.29 A significant feature of AES is its flexibility in supporting three different key sizes: 128 bits, 192 bits, and 256 bits.1 These varying key lengths offer different levels of security, with longer keys providing exponentially greater resistance against brute-force attacks.77
   The AES algorithm transforms plaintext into ciphertext through a series of repeated rounds. The number of rounds depends on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.[57] Each round involves several transformation steps, including byte substitution, shifting rows, mixing columns, and adding a round key derived from the main encryption key.[57] Unlike its predecessor DES, which is based on a Feistel network, AES employs a Substitution-Permutation Network (SPN) architecture, which is known for its strong security properties.[57] The selection of AES as the standard encryption algorithm was the result of a transparent and rigorous public competition conducted by NIST, which involved extensive scrutiny and analysis by cryptographers worldwide, fostering high confidence in its security and robustness against various cryptanalytic techniques.[52]
   AES plays a critical role in securing a wide range of network protocols within the

TCP/IP suite. In the Transport Layer, AES is the overwhelmingly preferred cipher suite for establishing secure HTTPS connections, ensuring the confidentiality of data exchanged between web browsers and servers.[1] NIST guidelines recommend AES cipher suites for TLS 1.2 and mandate support for TLS 1.3 with FIPS-based cipher suites that include AES.[98] At the Network Layer, AES is a strong encryption option within Internet Protocol Security (IPsec), which is used to secure Virtual Private Network (VPN) connections and other network layer communications.[13] Notably, the AES-GCM (Galois/Counter Mode) provides authenticated encryption for IPsec, offering both confidentiality and data integrity.[38] Furthermore, in the realm of wireless network security, the WPA2 and WPA3 standards utilize AES to encrypt data transmitted over Wi-Fi networks, ensuring the privacy of wireless communications.[13] Beyond these core protocols, AES finds application in various other areas, including file encryption, disk encryption for data at rest, securing sensitive data stored in databases, and in secure communication protocols such as Secure Shell (SSH) for remote access.[39] Due to its robust security and efficient performance in both software and hardware, AES has become the de facto standard for symmetric encryption across a wide spectrum of network protocols and applications, solidifying its position as a cornerstone of modern network security.[74]

The different key sizes supported by AES (128, 192, and 256 bits) have significant implications for the level of security they provide. Longer keys offer an exponentially greater level of security against brute-force attacks, making it computationally infeasible for attackers to try all possible key combinations.[77] AES-128 employs a 128-bit key and undergoes 10 rounds of encryption.[77] AES-192 utilizes a 192-bit key and 12 rounds.[77] The most secure variant, AES-256, uses a 256-bit key and 14 rounds of encryption. It is considered virtually uncrackable with currently available computing technology and is approved by the US government for protecting highly sensitive and classified information.[38] The choice of which AES key size to use typically depends on the sensitivity of the specific data being protected and the potential level of threat that needs to be mitigated.

5. Asymmetric Key Cryptography:
   Asymmetric key cryptography, also known as public-key cryptography, is a cryptographic system that utilizes two distinct but mathematically related keys for encryption and decryption.1 These two keys are referred to as the public key and the private key. The public key can be freely shared with anyone and is used for encryption purposes, while the private key is kept secret by its owner and is used for decryption.39 The fundamental principle behind asymmetric cryptography is that although the public and private keys are mathematically linked, it is

computationally infeasible to derive the private key from the public key.114
Asymmetric cryptography serves as the foundation for Public Key Infrastructure (PKI), a system that underpins many secure online interactions.107
Asymmetric key cryptography offers several advantages over symmetric key cryptography in the context of network security. One of the most significant benefits is that it elegantly solves the key distribution problem inherent in symmetric systems. Because the public key can be openly shared, there is no need for a secure channel to exchange secret keys between communicating parties.[1] Furthermore, asymmetric cryptography enables confidentiality when a sender encrypts a message using the recipient's public key, ensuring that only the holder of the corresponding private key can decrypt and read the message.[39]
Another crucial advantage of asymmetric cryptography is its ability to provide authentication and non-repudiation through the use of digital signatures. By signing a message with their private key, the sender can create a unique signature that can be verified by anyone using their corresponding public key, thus confirming the sender's identity and the integrity of the message.[13]
However, asymmetric cryptography also has certain disadvantages compared to its symmetric counterpart. One significant drawback is that it is generally slower and more computationally intensive than symmetric encryption.[1] This increased computational overhead makes it less suitable for encrypting large amounts of data directly. Additionally, for equivalent levels of security, asymmetric algorithms typically require larger key sizes compared to symmetric algorithms.[1]
Furthermore, asymmetric systems are susceptible to man-in-the-middle attacks if the authenticity of the public keys being exchanged is not properly verified.[110]
Due to the performance overhead associated with asymmetric encryption, it is often employed for key exchange and digital signatures, while symmetric encryption is generally preferred for the efficient encryption of bulk data once a secure session key has been established.[1]

6. The RSA Algorithm:
   The Rivest-Shamir-Adleman (RSA) algorithm is a widely recognized and utilized public-key cryptosystem that plays a crucial role in secure data transmission.153
   RSA is an asymmetric algorithm whose security is rooted in the mathematical difficulty of factoring the product of two very large prime numbers.153 The fundamental principle behind RSA is that while multiplying two large prime numbers together is a computationally straightforward task, reversing this process to find the original prime factors is extremely difficult, especially when the prime numbers are sufficiently large.153
   RSA finds numerous applications in network security protocols within the TCP/IP suite. One of its primary uses is for secure key exchange. In earlier versions of

TLS/SSL, RSA was commonly employed during the handshake process to encrypt and exchange the symmetric session keys that would then be used for the bulk encryption of data.[5] Another significant application of RSA is in the creation and verification of digital signatures. Digital signatures generated using RSA ensure both the integrity of the data and the authentication of the sender, providing a high level of trust in digital communications.[13] In essence, RSA is a versatile cryptographic tool used for both encryption and digital signatures, making it a fundamental component of numerous secure communication protocols.[153]

The RSA key generation process involves several steps. First, two large prime numbers, typically denoted as p and q, are chosen. These prime numbers should be selected randomly and be of significant size to make factorization difficult.[153] Next, the modulus n is calculated by multiplying these two primes: $n = p \times q$. The modulus n is used as part of both the public and private keys. Then, Euler's totient function, denoted as $\phi(n)$, is computed as $\phi(n) = (p - 1) \times (q - 1)$. A public exponent e is then chosen such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$, meaning their greatest common divisor is 1. Finally, the private exponent d is calculated as the modular multiplicative inverse of e modulo $\phi(n)$, which satisfies the equation $(d \times e) \mod \phi(n) = 1$. The public key consists of the modulus n and the public exponent e, while the private key consists of the modulus n and the private exponent d. For encryption, the sender uses the recipient's public key (n, e) to encrypt a message m into ciphertext c using the formula $c = m$^{e} mod n. For decryption, the recipient uses their private key (n, d) to recover the original message m from the ciphertext c using the formula $m = c$^{d} mod n.[153] The security of the RSA algorithm is heavily dependent on the size and the careful selection of the initial prime numbers, as the difficulty of factoring the large modulus n is what prevents unauthorized parties from deriving the private key from the publicly known information.[153]

7. The Diffie-Hellman Key Exchange Protocol:

   The Diffie-Hellman (DH) key exchange protocol is a cryptographic protocol that enables two parties, who may have no prior knowledge of each other, to establish a shared secret key over an insecure communication channel.13 This shared secret key can then be used to encrypt subsequent communications using a symmetric-key cipher, ensuring the privacy of the exchanged data.199 The security of the Diffie-Hellman protocol relies on the mathematical difficulty of the discrete logarithm problem, which makes it computationally hard for an eavesdropper to determine the shared secret even if they intercept all the public information exchanged.200

   The Diffie-Hellman key exchange enables two parties to establish a secure communication channel over a network without any prior exchange of secret

keys. The process begins with both parties, typically referred to as Alice and Bob, agreeing on two public parameters: a large prime number *p* (the modulus) and an integer *g* (the base or generator) which is a primitive root modulo *p*.[200] These values, *p* and *g*, can be transmitted over an insecure channel as their secrecy is not required for the security of the key exchange. Next, Alice chooses a secret integer *a* which she keeps private, and Bob independently chooses another secret integer *b*, also kept private.[200] Alice then computes her public value *A* as *A* = *g*^{*a*} mod *p*, and Bob computes his public value *B* as *B* = *g*^{*b*} mod *p*. These public values, *A* and *B*, are then exchanged over the insecure channel. Finally, Alice computes the shared secret key *s*_{*A*} by raising Bob's public value to her private secret: *s*_{*A*} = *B*^{*a*} mod *p*. Similarly, Bob computes the shared secret key *s*_{*B*} by raising Alice's public value to his private secret: *s*_{*B*} = *A*^{*b*} mod *p*. Through the properties of modular arithmetic, both Alice and Bob will arrive at the same shared secret key (*s*_{*A*} = *s*_{*B*} = *g*^{*ab*} mod *p*), even though their private secrets *a* and *b* have never been transmitted.[200] While the Diffie-Hellman key exchange is effective in establishing a shared secret, the basic protocol is vulnerable to man-in-the-middle (MITM) attacks because it does not provide any inherent mechanism for authentication of the communicating parties.[145] In a MITM attack, an adversary can intercept the public values exchanged between Alice and Bob, and establish separate shared secrets with each of them, effectively eavesdropping on their communication without either party being aware.[145] To address this vulnerability, modern variations of the Diffie-Hellman protocol have been developed that incorporate authentication mechanisms. One such variation is Elliptic Curve Diffie-Hellman (ECDH), which utilizes elliptic curve cryptography to achieve similar security with smaller key sizes and improved performance, making it suitable for resource-constrained environments.[114] Another important variation is Ephemeral Diffie-Hellman (DHE), where the public and private keys are generated anew for each communication session. This provides a property known as perfect forward secrecy, ensuring that even if an attacker were to compromise the long-term private key of one of the parties in the future, they would not be able to decrypt past communication sessions that used different ephemeral keys.[199]

8. Security Services in Computer Networking and the TCP/IP Suite:
   Security services in computer networking and the TCP/IP suite are essential to ensure secure communication and protect data from various threats. These services encompass several key principles: confidentiality, integrity, authentication, and non-repudiation.13
   Confidentiality aims to ensure that information is accessible only to authorized

users and is not disclosed to unauthorized individuals.[3] In the TCP/IP suite, confidentiality is primarily achieved through the use of encryption protocols. For example, TLS/SSL at the Transport Layer encrypts application data, making it unreadable to eavesdroppers.[222] Similarly, IPsec at the Network Layer encrypts IP packets, providing confidentiality for network traffic, often used in VPNs.[15]

Integrity focuses on ensuring the accuracy and completeness of data and preventing unauthorized modification or tampering.[8] Data integrity in the TCP/IP suite is maintained through mechanisms like digital signatures, which can verify the authenticity and integrity of data.[8] Message Authentication Codes (MACs) also serve to ensure data integrity by providing a cryptographic checksum that can detect alterations.[8] At the Transport Layer, TCP itself uses checksums and sequence numbers to ensure that data is delivered accurately and in the correct order.[8]

Authentication involves verifying the identity of the communicating entities, ensuring that the sender and receiver are who they claim to be.[1] Authentication in the TCP/IP suite can be achieved through various methods, including the use of passwords, biometric authentication, and digital certificates.[5] Protocols like CHAP (Challenge-Handshake Authentication Protocol) and EAP (Extensible Authentication Protocol) are used for authentication in certain TCP/IP scenarios.[237] At the Transport Layer, TLS/SSL uses digital certificates to authenticate the server and optionally the client.[5] IPsec also provides authentication of IP packets using Authentication Headers (AH) or through the Encapsulating Security Payload (ESP).[13]

Non-repudiation provides assurance that a sender cannot deny having sent a particular message or performed an action.[13] In the context of the TCP/IP suite, non-repudiation is typically achieved through the use of digital signatures. Because a digital signature is created using the sender's private key and can only be verified using their corresponding public key, it provides strong evidence that the message originated from that specific sender, and they cannot plausibly deny having sent it.[19]

These security services are fundamental to establishing trust and ensuring secure communication over potentially untrusted networks like the internet.[3]

9. Digital Signatures:

   Digital signatures are a cryptographic technique used to ensure data integrity and sender authentication in network communications, particularly within protocols of the TCP/IP suite.13 A digital signature is created using asymmetric cryptography, where the sender uses their private key to sign a message.19 Often, instead of signing the entire message, a cryptographic hash of the message is created first, and then this hash is signed. This is more efficient for long messages and also

ensures that the signature is of a fixed length.121 The resulting digital signature is then attached to the message and transmitted to the recipient.

The recipient of a digitally signed message can verify the signature using the sender's corresponding public key.[121] The verification process typically involves the recipient independently calculating the hash of the received message using the same hashing algorithm that the sender used. The recipient then decrypts the digital signature using the sender's public key to obtain the original hash value (or a value that should match the original hash). If the recipient's calculated hash matches the hash obtained from the signature, it confirms two crucial aspects of the communication. First, it authenticates the sender, providing assurance that the message originated from the owner of the private key used to create the signature. Second, it ensures the integrity of the data, as any alteration to the message after it was signed would result in a different hash value, causing the signature verification to fail.[121]

Digital signatures play a vital role in various protocols within the TCP/IP suite. For instance, in TLS/SSL, digital signatures are used to authenticate the server to the client during the handshake process, allowing the client to verify that it is indeed communicating with the legitimate server. Client authentication can also be achieved using digital signatures.[5] Digital signatures are also fundamental to non-repudiation, as they provide irrefutable proof of the sender's identity and the message's integrity at the time of signing.[19] Furthermore, digital signatures are used in other applications within the TCP/IP ecosystem, such as signing software code to verify its origin and integrity, and in securing email communications using protocols like PGP.[5]

10. Key Management in Network Environments:

Key management is a critical aspect of network security that encompasses the secure generation, distribution, storage, rotation, and revocation of cryptographic keys for both symmetric and asymmetric cryptography.13 Effective key management is essential because the security provided by even the strongest encryption algorithms can be completely undermined by weak or compromised keys.17 As the number of communicating parties within a network environment grows, the complexity of managing cryptographic keys also increases significantly, posing a challenge to scalability.33

Various techniques are employed for key generation, distribution, storage, and revocation in network environments for both symmetric and asymmetric cryptography.[7] For symmetric keys, secure channels are often used for the initial exchange, such as employing asymmetric encryption to protect the key during transmission. Key Distribution Centers (KDCs), like Kerberos, provide a centralized approach to managing and distributing symmetric keys within a domain.[13] Session

keys, which are temporary symmetric keys generated for a specific communication session, are commonly used to encrypt the bulk of data after an initial secure key exchange.[119] Implementing key rotation, where keys are periodically changed, is a crucial best practice to limit the potential damage if a key is compromised.[37] For asymmetric keys, Public Key Infrastructure (PKI) provides a framework for managing and distributing public keys, typically using Certificate Authorities (CAs) to verify the association between a public key and an identity.[33] Other models, like the web of trust used by PGP, offer decentralized key authentication.[33] For secure storage of cryptographic keys, Hardware Security Modules (HSMs) provide tamper-resistant environments.[37] A common approach in many secure systems is to use a hybrid approach, where asymmetric encryption is used for the secure exchange of a symmetric key, and then the symmetric key is used for the more efficient encryption of the bulk data.[1]

11. IP Security (IPsec):
    IP Security (IPsec) is a suite of protocols that provides a framework for securing IP communications by authenticating and encrypting each IP packet in a data stream.13 IPsec operates at the network layer (Layer 3) of the TCP/IP model, providing security services to all protocols above it.13 The IPsec architecture includes two primary protocols: the Authentication Header (AH) and the Encapsulating Security Payload (ESP).13
    The Authentication Header (AH) protocol provides data integrity and authentication for IP packets.[13] AH ensures that the data has not been tampered with during transmission and verifies the origin of the packet, confirming that it came from a trusted sender.[225] However, AH does not provide data confidentiality as it does not encrypt the payload of the IP packet.[15]
    The Encapsulating Security Payload (ESP) protocol, on the other hand, provides both data confidentiality through encryption and also offers integrity and authentication services.[13] ESP encrypts the payload of the IP packet, protecting it from eavesdropping, and it can also provide integrity and authentication similar to AH.[15] IPsec operates below the transport layer, meaning it can secure all IP traffic between selected endpoints, regardless of the application or protocol being used at higher layers.[15] A common application of IPsec is in creating secure Virtual Private Networks (VPNs) over public networks like the internet. In this context, IPsec encrypts all traffic between VPN gateways or between a VPN client and a VPN server, ensuring the privacy and security of the data being transmitted.[13]
    IPsec supports two main modes of operation: Tunnel Mode and Transport Mode.[15] In Tunnel Mode, the entire original IP packet, including both the header and the payload, is encrypted and authenticated. This encrypted packet is then encapsulated within a new IP packet with a new header. Tunnel Mode is primarily

used for creating VPNs, where secure tunnels are established between networks or between a host and a network.[15] In Transport Mode, only the payload of the IP packet is typically encrypted and/or authenticated. The original IP header remains intact, allowing for routing to occur normally. Transport Mode is often used for securing communication directly between specific hosts within a network.[15] The choice between Tunnel Mode and Transport Mode depends on the specific security requirements and the overall network architecture.

12. Secure Sockets Layer (SSL) and Transport Layer Security (TLS):
    Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptographic protocols that provide secure communication over a network, primarily at the transport layer (Layer 4) of the TCP/IP model.1 TLS is an updated and more secure version of the original SSL protocol.86 SSL/TLS is fundamental to securing web browsing, enabling HTTPS (HTTP over SSL/TLS), and is also used to secure other internet applications such as email, messaging, and VoIP.1
    SSL/TLS provides secure communication at the transport layer by encrypting the data transmitted between web browsers (clients) and web servers, ensuring both confidentiality and integrity.[1] Additionally, SSL/TLS authenticates the server to the client (and optionally the client to the server) using digital certificates, allowing the client to verify the identity of the website it is communicating with.[1]
    The establishment of a secure SSL/TLS connection begins with the SSL/TLS handshake process.[1] This process involves several steps between the client and the server, including the negotiation of the protocol version and the cipher suite to be used for the session. The cipher suite specifies the cryptographic algorithms for encryption, authentication, and key exchange.[1] Key exchange algorithms, such as RSA and Diffie-Hellman (including its elliptic curve variant ECDH), are used to securely establish the shared secret session keys that will be used for encrypting the data.[1] During the handshake, the server presents its digital certificate to the client, which the client verifies with a trusted Certificate Authority (CA) to authenticate the server's identity.[1]
13. Pretty Good Privacy (PGP):
    Pretty Good Privacy (PGP) is a widely adopted program designed to provide privacy and authentication for digital communications, particularly email.29 Its primary purpose is to secure email and other forms of digital communication over networks by ensuring confidentiality and authenticity of messages.110 PGP achieves this security by employing a combination of both symmetric and asymmetric encryption techniques.29
    When securing an email message using PGP, the program typically uses a symmetric encryption algorithm, such as AES, to encrypt the body of the email. This is done for efficiency, as symmetric encryption is generally faster for

encrypting large amounts of data.[40] The secret key used for this symmetric encryption is then itself encrypted using the recipient's public key, typically an RSA or ECC key. This ensures that only the intended recipient, who possesses the corresponding private key, can decrypt the symmetric key and thus access the original email content.[40]

In addition to providing confidentiality, PGP also enables sender authentication and data integrity through the use of digital signatures. The sender can use their private key to create a digital signature of the email message (or its hash), which is then attached to the email. The recipient can then use the sender's public key to verify the signature, confirming the sender's identity and ensuring that the message has not been altered during transit.[40] PGP traditionally relies on a "web of trust" model for authenticating public keys, where users digitally sign each other's public keys to indicate their trust in the key's owner's identity.[33]

14. Firewalls:

    Firewalls are a critical network security device that functions as a barrier between a trusted internal network and an untrusted external network, such as the internet.13 Their primary role is to control incoming and outgoing network traffic based on a set of predefined security rules.13 Firewalls are a fundamental component of network perimeter security, acting as the first line of defense against external threats.13

    Firewalls control network traffic by examining packets as they attempt to enter or leave the network. The rules configured on the firewall typically specify criteria based on various attributes of the network traffic, including the source and destination IP addresses, the source and destination port numbers, and the network protocol being used (e.g., TCP, UDP).[13] If a network packet matches a rule that permits the traffic, it is allowed to pass through. Conversely, if a packet matches a rule that denies the traffic, it is blocked. Many modern firewalls are stateful, meaning they can track the state of active network connections. This allows them to make more intelligent decisions about whether to allow traffic based on the context of the connection, rather than just examining individual packets.[224]

    There are different types of firewalls, each with its own characteristics and level of sophistication.[13] Packet filtering firewalls are the most basic type, operating by examining the headers of network packets and making decisions based on the information found there, such as source and destination IP addresses and port numbers.[223] Stateful firewalls, as mentioned earlier, maintain information about the state of active connections, allowing them to filter traffic more effectively. Application firewalls operate at a higher layer (the application layer) and can analyze the actual content of the network traffic, enabling them to block

malicious payloads or specific types of application-level attacks.[223]
Next-generation firewalls (NGFWs) integrate a wider range of security features beyond traditional firewall capabilities, such as intrusion detection and prevention systems (IDPS), deep packet inspection, and application control.[223] The different types of firewalls offer varying levels of inspection and control over network traffic, providing defense against a broad spectrum of network-based threats.

15. Conclusion:
This report has provided a comprehensive overview of key network security concepts within the context of Computer Networking and the TCP/IP suite. We have explored the fundamental principles of symmetric and asymmetric key cryptography, examining specific algorithms like DES, AES, RSA, and Diffie-Hellman, and their respective roles in securing network communications. We have also detailed the various security services crucial for protecting data in transit, including confidentiality, integrity, authentication, and non-repudiation, and the cryptographic techniques used to achieve them. Furthermore, we have discussed the importance and challenges of key management in network environments, as well as the functionality of essential network security protocols and devices such as IPsec, SSL/TLS, PGP, and firewalls.
The analysis indicates the interconnectedness of cryptography and network security protocols in establishing secure communication over the TCP/IP suite. Cryptographic algorithms provide the foundational tools for encryption, decryption, signing, and verification, while network security protocols integrate these tools to implement specific security services at different layers of the TCP/IP model. For instance, SSL/TLS leverages symmetric encryption for data confidentiality and asymmetric cryptography for key exchange and authentication at the Transport Layer, securing applications like web browsing. IPsec, operating at the Network Layer, utilizes encryption and authentication protocols to secure IP packets, often forming the basis for VPNs.
In network environments, adopting a layered security approach, often referred to as defense in depth, is crucial for providing comprehensive protection. This strategy involves utilizing a combination of cryptographic techniques, security protocols, and security devices, implemented at various points within the network infrastructure. By implementing multiple layers of security controls, organizations can increase their resilience against attacks and minimize the impact of potential security breaches.
Looking towards the future, the field of network security and cryptography continues to evolve to address emerging threats and technological advancements. One significant trend is the development of post-quantum cryptography. As quantum computing technology advances, many currently used

asymmetric key algorithms, such as RSA and ECC, are expected to become vulnerable to attacks. Post-quantum cryptographic algorithms are being researched and developed to provide security against both classical and quantum computers, ensuring the continued protection of sensitive data in the future.

Key Valuable Tables:

1. **Comparison of Symmetric and Asymmetric Key Cryptography:**

Feature	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key Type	Single secret key	Public and private key pair
Key Usage	Same key for encryption and decryption	Public key for encryption, private key for decryption
Key Sharing	Requires secure sharing of the secret key	Public key can be freely shared
Speed	Faster and more efficient for large amounts of data	Slower and more computationally intensive
Security Level	Security relies on the secrecy of the single key	Security relies on the secrecy of the private key
Common Algorithms	AES, DES, 3DES, RC4	RSA, ECC, Diffie-Hellman
Primary Use Cases	Bulk data encryption, VPNs, secure data storage, internal comms	Secure key exchange, digital signatures, authentication, secure email

2. **Summary of Security Services in TCP/IP:**

Security Service	Definition	How Achieved in TCP/IP
Confidentiality	Ensuring information is accessible only to authorized users	Encryption protocols like AES in TLS/SSL and IPsec
Integrity	Ensuring data accuracy and preventing unauthorized	Digital signatures (RSA, DSA,

	modification	ECC), MACs, TCP checksums
Authentication	Verifying the identity of communicating entities	Digital certificates in TLS/SSL, IPsec authentication headers, password-based auth
Non-Repudiation	Preventing a sender from denying that they sent a particular message/action	Digital signatures (RSA, DSA, ECC)

3. **Common Cryptographic Algorithms and Their Applications in TCP/IP:**

Algorithm	**Type**	**Key Applications in TCP/IP**
DES	Symmetric	Legacy encryption
AES	Symmetric	TLS/SSL, IPsec, Wi-Fi security (WPA2/3), PGP, file/disk encryption, SSH
RSA	Asymmetric	Key exchange (older TLS/SSL), digital signatures, PGP
Diffie-Hellman/ECDH	Asymmetric	Key exchange in TLS/SSL and IPsec (provides forward secrecy with ephemeral variants)

Works cited

1. Appendix A Introduction to Public-Key Cryptography, accessed on April 21, 2025, https://docs.oracle.com/cd/E19263-01/817-5215/ax_crypt.html
2. www.ibm.com, accessed on April 21, 2025, https://www.ibm.com/docs/SSGMCP_5.5.0/security/tcpip/dfht5nh.html#:~:text=TCP%2FIP%20connections%20between%20clients,between%20the%20client%20and%20server.
3. About security for TCP/IP clients - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/SSGMCP_5.5.0/security/tcpip/dfht5nh.html
4. Does TCP/IP expose critical infrastructure to added risk?, accessed on April 21, 2025, https://security.stackexchange.com/questions/19218/does-tcp-ip-expose-critical-infrastructure-to-added-risk

5. uregina.ca, accessed on April 21, 2025, https://uregina.ca/~kozdron/Teaching/Regina/124Winter09/Handouts/secure_webpages.pdf
6. Which Internet Protocol is Used to Transmit Encrypted Data: A Clear Explanation, accessed on April 21, 2025, https://www.berylliuminfosec.com/blog/which-internet-protocol-is-used-to-transmit-encrypted-data-60e06
7. Exploring TCP/IP Model: The Layer For Data Formatting, Compression, And Encryption, accessed on April 21, 2025, https://www.newsoftwares.net/blog/exploring-tcp-ip-model-the-layer-for-data-formatting-compression-and-encryption/
8. TCP/IP Model | GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/tcp-ip-model/
9. TCP/IP model | Network Security and Forensics Class Notes - Fiveable, accessed on April 21, 2025, https://library.fiveable.me/network-security-and-forensics/unit-2/tcpip-model/study-guide/GtrEKXqG86dcXt1Y
10. Network Security in the TCP/IP Model vs. OSI Model - Abusix, accessed on April 21, 2025, https://abusix.com/blog/network-security-in-the-tcp-ip-model-vs-osi-model/
11. What is TCP/IP? The communication model explained | A1 Digital, accessed on April 21, 2025, https://www.a1.digital/news/tcp-ip-explained/
12. What is the TCP/IP Model? The Internet Protocol Suite - Simplilearn.com, accessed on April 21, 2025, https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-tcp-ip-model
13. 18, accessed on April 21, 2025, https://faculty.utrgv.edu/john.abraham/6345/new%20ppt/30-network%20security.ppt
14. Security for TCP/IP clients - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/en/cics-ts/6.x?topic=layers-security-tcpip-clients
15. IPsec - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/IPsec
16. Security - UTRGV Faculty Web, accessed on April 21, 2025, https://faculty.utrgv.edu/john.abraham/4345/ppt/30-network%20security.ppt
17. What Is Symmetric Encryption? - IBM, accessed on April 21, 2025, https://www.ibm.com/think/topics/symmetric-encryption
18. Cryptography and Network Security: Ensuring Confidentiality and ..., accessed on April 21, 2025, https://www.institutedata.com/us/blog/cryptography-and-network-security/
19. Cryptography Supporting Confidentiality — MCSI Library, accessed on April 21, 2025, https://library.mosse-institute.com/articles/2023/07/cryptography-supporting-confidentiality.html
20. keys - Why does symmetric encryption not provide authentication ..., accessed on April 21, 2025,

https://crypto.stackexchange.com/questions/108494/why-does-symmetric-encryption-not-provide-authentication-and-integrity-is-it-on
21. No Slide Title, accessed on April 21, 2025, https://condor.depaul.edu/~jtullis/Q2_ECT581/wk3/Security.ppt
22. What is Non-repudiation in Cyber Security? | Bitsight, accessed on April 21, 2025, https://www.bitsight.com/glossary/non-repudiation-cyber-security
23. Network Security - NMT Computer Science and Engineering, accessed on April 21, 2025, https://www.cs.nmt.edu/~cs353/Lectures/Lecture_21_IPSec.pdf
24. 4.1: Accountability - Engineering LibreTexts, accessed on April 21, 2025, https://eng.libretexts.org/Courses/Delta_College/Information_Security/04%3A_Auditing_and_Accountability/4.1%3A_Accountability
25. Security Services in Information Security - Digitdefence, accessed on April 21, 2025, https://digitdefence.com/blog/security-services-in-information-security
26. What is a Symmetric Key? - Thales, accessed on April 21, 2025, https://cpl.thalesgroup.com/faq/key-secrets-management/what-symmetric-key
27. cpl.thalesgroup.com, accessed on April 21, 2025, https://cpl.thalesgroup.com/faq/key-secrets-management/what-symmetric-key#:~:text=In%20cryptography%2C%20a%20symmetric%20key,was%20used%20to%20encrypt%20it.
28. What is Symmetric Key Cryptography? | Security Encyclopedia - HYPR, accessed on April 21, 2025, https://www.hypr.com/security-encyclopedia/symmetric-key-cryptography
29. What is Symmetric Key Cryptography Encryption? | Security Wiki - Secret Double Octopus, accessed on April 21, 2025, https://doubleoctopus.com/security-wiki/encryption-and-cryptography/symmetric-key-cryptography/
30. symmetric key - Glossary | CSRC - NIST Computer Security Resource Center, accessed on April 21, 2025, https://csrc.nist.gov/glossary/term/symmetric_key
31. Symmetric Cryptography - Glossary | CSRC - NIST Computer Security Resource Center, accessed on April 21, 2025, https://csrc.nist.gov/glossary/term/symmetric_cryptography
32. Symmetric key cryptography - IBM Quantum Learning, accessed on April 21, 2025, https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/symmetric-key-cryptography
33. Symmetric-key algorithm - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Symmetric-key_algorithm
34. 8.2 Symmetric Key Cryptography, accessed on April 21, 2025, https://math-sites.uncg.edu/sites/pauli/112/HTML/secsymcrypto.html
35. Symmetric Key Cryptography | GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/symmetric-key-cryptography/
36. faculty.utrgv.edu, accessed on April 21, 2025, https://faculty.utrgv.edu/john.abraham/6345/new%20ppt/30-network%20security.ppt#:~:text=In%20symmetric%2Dkey%20cryptography%2C%20the,The%20key%20is%20shared.&text=*-,In%20symmetric%2Dkey%20cryptography%2C%20th

e%20same%20key.is%20used%20in%20both%20directions.&text=Takes%2064%2Dbit%20plaintext%20and%20creates%20a%2064%2Dbit%20ciphertext.
37. What is symmetric encryption? | Entrust, accessed on April 21, 2025, https://www.entrust.com/resources/learn/symmetric-encryption
38. What Is Data Encryption? - Palo Alto Networks, accessed on April 21, 2025, https://www.paloaltonetworks.com/cyberpedia/data-encryption
39. Difference Between Symmetric and Asymmetric Key Encryption | GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/
40. When to Use Symmetric vs Asymmetric Encryption | Venafi - Machine Identity Security, accessed on April 21, 2025, https://venafi.com/blog/what-are-best-use-cases-symmetric-vs-asymmetric-encryption/
41. hash - Does symmetric encryption provide data integrity ..., accessed on April 21, 2025, https://security.stackexchange.com/questions/9437/does-symmetric-encryption-provide-data-integrity
42. About IPSec Algorithms and Protocols - WatchGuard, accessed on April 21, 2025, http://www.watchguard.com/help/docs/help-center/en-US/content/en-US/Firebox/mvpn/general/ipsec_algorithms_protocols_c.html
43. The IPsec VPN must use Advanced Encryption Standard (AES) encryption for the IPsec proposal to protect the confidentiality of remote access sessions. - STIG Viewer, accessed on April 21, 2025, https://www.stigviewer.com/stig/virtual_private_network_vpn_security_requirements_guide/2021-03-25/finding/V-207257
44. RFC 3686 - Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP) - IETF Datatracker, accessed on April 21, 2025, https://datatracker.ietf.org/doc/html/rfc3686
45. New IPSec Traffic Forwarding Guidance for Zscaler Customers, accessed on April 21, 2025, https://www.zscaler.com/blogs/product-insights/new-ipsec-traffic-forwarding-guidance-zscaler-customers
46. EtherNet/IP Security: Encryption Basics - Real Time Automation, Inc., accessed on April 21, 2025, https://www.rtautomation.com/rtas-blog/ethernet-ip-security-encryption-basics/
47. HISTORY OF DES, accessed on April 21, 2025, https://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/des%20history.html
48. Data Encryption Standard - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Data_Encryption_Standard
49. History of DES Encryption - Tutorialspoint, accessed on April 21, 2025, https://www.tutorialspoint.com/what-is-the-history-of-des
50. Lecture 4 Data Encryption Standard (DES), accessed on April 21, 2025, https://www.lri.fr/~fmartignon/documenti/systemesecurite/4-DES.pdf

51. Data Encryption Standard (DES) | Set 1 - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/
52. Data Encryption Standard (DES) Algorithm in Cryptography - Simplilearn.com, accessed on April 21, 2025, https://www.simplilearn.com/what-is-des-article
53. Advantages and Disadvantages of DES - Tutorialspoint, accessed on April 21, 2025, https://www.tutorialspoint.com/what-are-the-advantage-and-disadvantage-of-des
54. The Data Encryption Standard (DES) and its strength against attacks, accessed on April 21, 2025, https://people.clarkson.edu/class/cs456/CoppersmithDES.pdf
55. DES Full Form - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/des-full-form/
56. Why Advanced Encryption Standard (AES) has replaced DES, 3DES and TDEA - Precisely, accessed on April 21, 2025, https://www.precisely.com/blog/data-security/aes-vs-des-encryption-standard-3des-tdea
57. Difference Between AES and DES Ciphers, accessed on April 21, 2025, https://www.shiksha.com/online-courses/articles/difference-between-aes-and-des-ciphers-blogId-158769
58. Data Encryption Standard (DES) - Britannica, accessed on April 21, 2025, https://www.britannica.com/topic/Data-Encryption-Standard
59. History of Cryptography, behind the code - Episode 4, accessed on April 21, 2025, https://www.theqrl.org/blog/history-of-cryptography-behind-the-code-part-4/
60. www.thalesgroup.com, accessed on April 21, 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption#:~:text=In%20the%20early%201970s%3A%20IBM,until%20it%20cracked%20in%201997.
61. A brief history of encryption (and cryptography) - Thales, accessed on April 21, 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption
62. The Cornerstone of Cybersecurity – Cryptographic Standards and a 50-Year Evolution, accessed on April 21, 2025, https://www.nccoe.nist.gov/news-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution
63. Decoding the Data Encryption Standard: What You Need to Know - Trustworthy, accessed on April 21, 2025, https://www.trustworthy.com/blog/decoding-the-data-encryption-standard
64. Difference between AES and DES ciphers - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/difference-between-aes-and-des-ciphers/
65. Difference Between AES and DES Ciphers - Tutorialspoint, accessed on April 21, 2025, https://www.tutorialspoint.com/difference-between-aes-and-des-ciphers
66. www.simplilearn.com, accessed on April 21, 2025, https://www.simplilearn.com/what-is-des-article#:~:text=The%20disadvantages%20of%20the%20DES,is%20available%20in%20the%20market.

67. Limitations Of Des - FasterCapital, accessed on April 21, 2025, https://fastercapital.com/topics/limitations-of-des.html
68. DES strength and weakness - Cryptography Stack Exchange, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/43544/des-strength-and-weakness
69. What is the main limitation of DES? - Cryptography Stack Exchange, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/56033/what-is-the-main-limitation-of-des
70. Advanced Encryption Standard Vs Data Encryption Standard | AES Vs. DES - AxCrypt, accessed on April 21, 2025, https://axcrypt.net/blog/advanced-encryption-standard-vs-data-encryption-standard/
71. Comparison of DES, Triple DES, AES, blowfish encryption for data - Stack Overflow, accessed on April 21, 2025, https://stackoverflow.com/questions/5554526/comparison-of-des-triple-des-aes-blowfish-encryption-for-data
72. is DES Faster Than AES on software - Cryptography Stack Exchange, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/50442/is-des-faster-than-aes-on-software
73. 3DES vs AES: Which Algorithm Should You Use? - CData Software, accessed on April 21, 2025, https://www.cdata.com/blog/3des-vs-aes
74. Advanced Encryption Standard (AES) - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/advanced-encryption-standard-aes/?ref=rp
75. AES Encryption: How it works, Benefits, and Use Cases - Splashtop, accessed on April 21, 2025, https://www.splashtop.com/blog/aes-encryption
76. What Is AES Encryption And How Does It Work? | JSCAPE, accessed on April 21, 2025, https://www.jscape.com/blog/aes-encryption
77. What is Advanced Encryption Standard (AES)? - Portnox, accessed on April 21, 2025, https://www.portnox.com/cybersecurity-101/what-is-advanced-encryption-standard-aes/
78. AES | Advanced Encryption Standard Engine IP Core - CAST, Inc., accessed on April 21, 2025, https://www.cast-inc.com/security/encryption-primitives/aes
79. Everything You Need to Know About AES-256 Encryption - Kiteworks, accessed on April 21, 2025, https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/
80. Advanced Encryption Standard (AES): What It Is and How It Works - The SSL Store, accessed on April 21, 2025, https://www.thesslstore.com/blog/advanced-encryption-standard-aes-what-it-is-and-how-it-works/
81. Advanced Encryption Standard (AES) - NIST Technical Series Publications, accessed on April 21, 2025,

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf
82. Supported encryption algorithms for IPsec VPNs - Next-Generation Firewall (NGFW), accessed on April 21, 2025, https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.9.0/GUID-E0FD9A38-F98A-45C0-AD83-E39CECF8CB9D.html
83. Why Encryption Algorithms GCMAES128, GCMAES192 and GCMAES256 are in the list of IKE-Phase2 IPsec Integrity drop-down list - Learn Microsoft, accessed on April 21, 2025, https://learn.microsoft.com/en-us/answers/questions/1061655/why-encryption-algorithms-gcmaes128-gcmaes192-and
84. IPSEC encryption: GCMAES256 versus AES256+SHA256 : r/networking - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/networking/comments/zlv4fb/ipsec_encryption_gcmaes256_versus_aes256sha256/
85. Using AES in CTR for TCP/IP based network connections - need to encrypt the IVs?, accessed on April 21, 2025, https://security.stackexchange.com/questions/80149/using-aes-in-ctr-for-tcp-ip-based-network-connections-need-to-encrypt-the-ivs
86. TLS vs. SSL: What's the Difference? - Rublon, accessed on April 21, 2025, https://rublon.com/blog/tls-vs-ssl-whats-the-difference/
87. Transport Layer Security - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Transport_Layer_Security
88. TLS and SSL - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/en/zos/2.4.0?topic=protocols-tls-ssl
89. Enhanced Security: AES-256 Encryption for SSL and TLS - LuxSci, accessed on April 21, 2025, https://luxsci.com/blog/256-bit-aes-encryption-for-ssl-and-tls-maximal-security.html
90. Security 101 for developers: TCP/IP, SSL/TLS Certificates, AES/CBC Encryption, Password Storage, and More - DEV Community, accessed on April 21, 2025, https://dev.to/ssd/security-101-for-developers-tcpip-ssltls-certificates-aescbc-encryption-password-storage-and-more-3cnn
91. AES vs SSL/TLS: Encryption for the internet of things - Electronic Products, accessed on April 21, 2025, https://www.electronicproducts.com/aes-vs-ssl-tls-encryption-for-the-internet-of-things/
92. What's the point of encrypting data at rest in the application-level with AES/RSA encryptions if I'm already using HTTPS? : r/node - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/node/comments/1dhtftk/whats_the_point_of_encrypting_data_at_rest_in_the/
93. Use ChaCha encryption algorithms instead of AES for HTTPS - Seafile Forum, accessed on April 21, 2025, https://forum.seafile.com/t/use-chacha-encryption-algorithms-instead-of-aes-for-https/14201

94. IIS8 - HTTPS connection using AES 128 - How to improve? - Server, accessed on April 21, 2025, https://community.letsencrypt.org/t/iis8-https-connection-using-aes-128-how-to-improve/41810
95. Applying manual AES encryption instead of using HTTPS - Stack Overflow, accessed on April 21, 2025, https://stackoverflow.com/questions/13568731/applying-manual-aes-encryption-instead-of-using-https
96. How to set up SSL (TLS) / HTTPS on Spring Boot using AES-256? - Stack Overflow, accessed on April 21, 2025, https://stackoverflow.com/questions/30404579/how-to-set-up-ssl-tls-https-on-spring-boot-using-aes-256
97. Sending Encryption/Decryption keys over HTTPS - Information Security Stack Exchange, accessed on April 21, 2025, https://security.stackexchange.com/questions/185166/sending-encryption-decryption-keys-over-https
98. Release of NIST Special Publication 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer S, accessed on April 21, 2025, https://csrc.nist.rip/publications/nistbul/itlbul2014_04.pdf
99. SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations | CSRC, accessed on April 21, 2025, https://csrc.nist.gov/pubs/sp/800/52/r2/final
100. TLS Guidelines: NIST Publishes SP 800-52 Revision 2 | CSRC, accessed on April 21, 2025, https://csrc.nist.gov/news/2019/nist-publishes-sp-800-52-revision-2
101. Acceptable Encryption Products and Algorithms - Information Technology - University of Florida, accessed on April 21, 2025, https://it.ufl.edu/security/security-guidance/acceptable-encryption-products-and-algorithms/
102. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations - NIST Technical Series Publications, accessed on April 21, 2025, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
103. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations - NIST Technical Series Publications, accessed on April 21, 2025, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-52r1.pdf
104. Recommended Cipher Suites for TLS 1.0, 1.1 and 1.2 - Information Security Stack Exchange, accessed on April 21, 2025, https://security.stackexchange.com/questions/11439/recommended-cipher-suites-for-tls-1-0-1-1-and-1-2
105. Test for conformance to NIST SP 800-52 · Issue #333 - GitHub, accessed on April 21, 2025, https://github.com/drwetter/testssl.sh/issues/333
106. IP/Network - ShareTechnote, accessed on April 21, 2025, https://www.sharetechnote.com/html/Handbook_IP_Network_Confidentiality_Integrity.html

107. cpl.thalesgroup.com, accessed on April 21, 2025, https://cpl.thalesgroup.com/faq/key-secrets-management/what-asymmetric-key-or-asymmetric-key-cryptography#:~:text=Asymmetric%20keys%20are%20the%20foundation,kept%20private%20(private%20key).
108. What is an Asymmetric Key or Asymmetric Key Cryptography? - Thales, accessed on April 21, 2025, https://cpl.thalesgroup.com/faq/key-secrets-management/what-asymmetric-key-or-asymmetric-key-cryptography
109. asymmetric cryptography - Glossary | CSRC - NIST Computer Security Resource Center, accessed on April 21, 2025, https://csrc.nist.gov/glossary/term/asymmetric_cryptography
110. Public-key cryptography - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Public-key_cryptography
111. What is Asymmetric Encryption? - IBM, accessed on April 21, 2025, https://www.ibm.com/think/topics/asymmetric-encryption
112. Asymmetric Encryption: Definition, Architecture, Usage - Okta, accessed on April 21, 2025, https://www.okta.com/identity-101/asymmetric-encryption/
113. What is asymmetric encryption? | Asymmetric vs. symmetric encryption - Cloudflare, accessed on April 21, 2025, https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/
114. Asymmetric Key Cryptography | GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/asymmetric-key-cryptography/
115. Asymmetric-key cryptography - Glossary | CSRC - NIST Computer Security Resource Center, accessed on April 21, 2025, https://csrc.nist.gov/glossary/term/asymmetric_key_cryptography
116. Asymmetric Encryption: What It Is and When to Use It | Venafi - Machine Identity Security, accessed on April 21, 2025, https://venafi.com/blog/what-asymmetric-encryption-is-and-when-to-use-it/
117. What is an Asymmetric Encryption? - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/what-is-asymmetric-encryption/
118. Exploring the Benefits and Challenges of Asymmetric Key Cryptography - Zeeve, accessed on April 21, 2025, https://www.zeeve.io/blog/exploring-the-benefits-and-challenges-of-asymmetric-key-cryptography/
119. Symmetric vs. Asymmetric Encryption: What's the Difference? - Trenton Systems, accessed on April 21, 2025, https://www.trentonsystems.com/en-gb/blog/symmetric-vs-asymmetric-encryption
120. Symmetric Encryption vs Asymmetric Encryption: How it Works and Why it's Used, accessed on April 21, 2025, https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/
121. Asymmetric Encryption: Benefits, Drawbacks & Use Cases - 1Kosmos, accessed on April 21, 2025, https://www.1kosmos.com/digital-identity-101/encryption/asymmetric-encryption/

122. Symmetric vs. Asymmetric Encryption - What are differences? - Cheap SSL Certificates, accessed on April 21, 2025, https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
123. When to Use Symmetric Encryption vs Asymmetric Encryption - Keyfactor, accessed on April 21, 2025, https://www.keyfactor.com/blog/symmetric-vs-asymmetric-encryption/
124. Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems, accessed on April 21, 2025, https://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf
125. Symmetric vs. Asymmetric Encryption: What's the Difference? - Trenton Systems, accessed on April 21, 2025, https://www.trentonsystems.com/en-us/resource-hub/blog/symmetric-vs-asymmetric-encryption
126. Symmetric Vs Asymmetric Encryption | Which Is More Secure, accessed on April 21, 2025, https://www.encryptionconsulting.com/symmetric-vs-asymmetric-encryption-which-is-more-secure/
127. Asymmetric key cryptography - IBM Quantum Learning, accessed on April 21, 2025, https://learning.quantum.ibm.com/course/practical-introduction-to-quantum-safe-cryptography/asymmetric-key-cryptography
128. How does public key cryptography work? | Public key encryption and SSL - Cloudflare, accessed on April 21, 2025, https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/
129. Asymmetric-Key Encryption and Digital Signatures in Practice - sergioprado.blog, accessed on April 21, 2025, https://sergioprado.blog/asymmetric-key-encryption-and-digital-signatures-in-practice/
130. ELI5: How encryption with asymmetric keys works? : r/explainlikeimfive - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/explainlikeimfive/comments/1bmvqc3/eli5_how_encryption_with_asymmetric_keys_works/
131. Using Asymmetric Keys – Practical Networking .net, accessed on April 21, 2025, https://www.practicalnetworking.net/series/cryptography/using-asymmetric-keys/
132. Digital signatures | Cloud KMS, accessed on April 21, 2025, https://cloud.google.com/kms/docs/digital-signatures
133. Understanding Digital Signatures | CISA, accessed on April 21, 2025, https://www.cisa.gov/news-events/news/understanding-digital-signatures
134. Asymmetric Cryptography - Xiphera, accessed on April 21, 2025, https://xiphera.com/asymmetric-cryptography/
135. Role of digital signatures in asymmetric cryptography - Infosec, accessed on April 21, 2025,

https://www.infosecinstitute.com/resources/cryptography/role-of-digital-signatures-in-asymmetric-cryptography/
136. Digital signatures | Microsoft Learn, accessed on April 21, 2025, https://learn.microsoft.com/en-us/devsecops/playbook/capabilities/security/signing
137. OCC 1999-20 Appendix A - Digital Signatures with Public Key Cryptography, accessed on April 21, 2025, https://www.occ.treas.gov/news-issuances/bulletins/1999/bulletin-1999-20a.pdf
138. Asymmetric algorithms — Cryptography 45.0.0.dev1 documentation, accessed on April 21, 2025, https://cryptography.io/en/latest/hazmat/primitives/asymmetric/
139. Asymmetric Authentication - Use Case Example - Developer Help, accessed on April 21, 2025, https://developerhelp.microchip.com/xwiki/bin/view/applications/security/asymmetric-use-case-example/
140. A Complete Guide to Asymmetric Encryption: Definition & Uses - Dashlane, accessed on April 21, 2025, https://www.dashlane.com/blog/complete-guide-to-asymmetric-encryption
141. What's the Difference Between Symmetric vs Asymmetric Encryption? - Trustifi, accessed on April 21, 2025, https://trustifi.com/blog/difference-between-symmetric-vs-asymmetric-encryption/
142. Symmetric vs Assymmetric Keys with Cell-Level Encryption - Microsoft Q&A, accessed on April 21, 2025, https://learn.microsoft.com/en-us/answers/questions/735107/symmetric-vs-assymmetric-keys-with-cell-level-encr
143. Asymmetric vs symmetric encryption benchmarks - Information Security Stack Exchange, accessed on April 21, 2025, https://security.stackexchange.com/questions/57493/asymmetric-vs-symmetric-encryption-benchmarks
144. What are sources for the performance difference in asymmetric and symmetric encryption?, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/66613/what-are-sources-for-the-performance-difference-in-asymmetric-and-symmetric-encr
145. How does the man in the middle attack work in Diffie–Hellman? - Stack Overflow, accessed on April 21, 2025, https://stackoverflow.com/questions/10471009/how-does-the-man-in-the-middle-attack-work-in-diffie-hellman
146. How to exploit Diffie-hellman to perform a man in the middle attack - Stack Overflow, accessed on April 21, 2025, https://stackoverflow.com/questions/9953187/how-to-exploit-diffie-hellman-to-perform-a-man-in-the-middle-attack
147. 14 Diffie–Hellman Key Exchange - sandilands.info, accessed on April 21, 2025, https://sandilands.info/crypto/DiffieHellmanKeyExchange.html
148. The Man in the Middle – Defend Dissent - Oregon State University, accessed

on April 21, 2025, https://open.oregonstate.education/defenddissent/chapter/the-man-in-the-middle/
149. What is a man-in-the-middle attack (for instance in Diffie-Hellman)? - Cryptography Stack Exchange, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/26669/what-is-a-man-in-the-middle-attack-for-instance-in-diffie-hellman
150. Man in the Middle attack in Diffie-Hellman Key Exchange | GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/man-in-the-middle-attack-in-diffie-hellman-key-exchange/
151. Man-in-the-Middle Attack on D-H Key Exchange - YouTube, accessed on April 21, 2025, https://www.youtube.com/watch?v=vdNwM8_cMo8
152. Diffie-Hellman and man-in-the-middle attacks - Cryptography Stack Exchange, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/19203/diffie-hellman-and-man-in-the-middle-attacks
153. RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained, accessed on April 21, 2025, https://www.splunk.com/en_us/blog/learn/rsa-algorithm-cryptography.html
154. RSA Encryption | Brilliant Math & Science Wiki, accessed on April 21, 2025, https://brilliant.org/wiki/rsa-encryption/
155. RSA cryptosystem - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/RSA_cryptosystem
156. RSA Algorithm in Cryptography - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
157. cybertalents.com, accessed on April 21, 2025, https://cybertalents.com/blog/rsa-encryption#:~:text=The%20RSA%20encryption%20process%20typically,decrypted%20with%20a%20private%20key.
158. RSA Encryption and RSA Algorithm: A Comprehensive Overview - CyberTalents, accessed on April 21, 2025, https://cybertalents.com/blog/rsa-encryption
159. Understanding RSA Asymmetric Encryption: How It Works - SecureW2, accessed on April 21, 2025, https://www.securew2.com/blog/what-is-rsa-asymmetric-encryption
160. RSA Algorithm: Secure Your Data with Public-Key Encryption - Simplilearn.com, accessed on April 21, 2025, https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm
161. Diffie-Hellman Key Exchange Vs. RSA | Encryption Consulting, accessed on April 21, 2025, https://www.encryptionconsulting.com/diffie-hellman-key-exchange-vs-rsa/
162. How does the RSA digital signature algorithm work, and what are the mathematical principles that ensure its security and reliability? - EITCA Academy, accessed on April 21, 2025, https://eitca.org/cybersecurity/eitc-is-acc-advanced-classical-cryptography/digit

al-signatures/digital-signatures-and-security-services/examination-review-digital-signatures-and-security-services/how-does-the-rsa-digital-signature-algorithm-work-and-what-are-the-mathematical-principles-that-ensure-its-security-and-reliability/
163. What are the steps involved in the key generation process of the RSA cryptosystem, and why is the selection of large prime numbers crucial? - EITCA Academy, accessed on April 21, 2025, https://eitca.org/cybersecurity/eitc-is-ccf-classical-cryptography-fundamentals/introduction-to-public-key-cryptography/the-rsa-cryptosystem-and-efficient-exponentiation/examination-review-the-rsa-cryptosystem-and-efficient-exponentiation/what-are-the-steps-involved-in-the-key-generation-process-of-the-rsa-cryptosystem-and-why-is-the-selection-of-large-prime-numbers-crucial/
164. RSA ENCRYPTION OF TCP MESSAGE - Asif Karim, accessed on April 21, 2025, https://asifkarim.com/wp-content/uploads/2019/11/a-cryptographic-application-for-secure-information-transfer-in-a-linux-network-environment.pdf
165. Cryptography in Everyday Life - LAITS, accessed on April 21, 2025, https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life
166. Encrypting client/server communications over TCP/IP - Sybase Infocenter, accessed on April 21, 2025, https://infocenter.sybase.com/help/topic/com.sybase.help.sqlanywhere.12.0.0/dbadmin/encrypting-tcpip-network.html
167. How does TLS work (RSA, Diffie-Hellman, PFS)? - Information Security Stack Exchange, accessed on April 21, 2025, https://security.stackexchange.com/questions/205639/how-does-tls-work-rsa-diffie-hellman-pfs
168. Lab 11: Experiment with RSA - CSCI 363 — Computer Networks -- Labs, accessed on April 21, 2025, http://www.eg.bucknell.edu/~cs363/2016-spring/labs/lab11-experiment-rsa.html
169. Managing Servers with Netscape Console: Introduction to Public-Key Cryptography, accessed on April 21, 2025, https://docs.oracle.com/cd/E19957-01/816-5567-10/app_cryp.htm
170. Do I understand correctly how to encrypt TCP traffic via RSA + AES? - Stack Overflow, accessed on April 21, 2025, https://stackoverflow.com/questions/63819977/do-i-understand-correctly-how-to-encrypt-tcp-traffic-via-rsa-aes
171. auth0.com, accessed on April 21, 2025, https://auth0.com/blog/the-tls-handshake-explained/#:~:text=The%20RSA%20key%20exchange%20works,ClientHello%20message%20to%20the%20server.
172. The TLS Handshake Explained - Auth0, accessed on April 21, 2025, https://auth0.com/blog/the-tls-handshake-explained/
173. When is an RSA key used in TLS handshake? - Information Security Stack Exchange, accessed on April 21, 2025, https://security.stackexchange.com/questions/205184/when-is-an-rsa-key-used-in-tls-handshake
174. TLS Handshake - OSDev Wiki, accessed on April 21, 2025,

https://wiki.osdev.org/TLS_Handshake
175. What happens in a TLS handshake? | SSL handshake - Cloudflare, accessed on April 21, 2025, https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/
176. Taking a Closer Look at the SSL/TLS Handshake, accessed on April 21, 2025, https://www.thesslstore.com/blog/explaining-ssl-handshake/
177. TLS/SSL .. DH vs RSA for key exchange and authentication? : r/AskNetsec - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/AskNetsec/comments/8nw0ik/tlsssl_dh_vs_rsa_for_key_exchange_and/
178. The TLS 1.2 Protocol - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/en/cloud-paks/z-modernization-stack/2023.4?topic=handshake-tls-12-protocol
179. RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol - IETF, accessed on April 21, 2025, https://www.ietf.org/rfc/rfc4432.txt
180. Key Exchange in SSL/TLS: Understanding RSA, Diffie-Hellman, and Elliptic Curves - Tech Papers - Citrix Community, accessed on April 21, 2025, https://community.citrix.com/tech-zone/build/tech-papers/key-exchange-in-ssl-tls/
181. RSA Key Exchange Attack [closed], accessed on April 21, 2025, https://crypto.stackexchange.com/questions/103276/rsa-key-exchange-attack
182. Diffie-Hellman vs RSA: How These Encryption Algorithms Differ - Machine Identity Security, accessed on April 21, 2025, https://venafi.com/blog/how-diffie-hellman-key-exchange-different-rsa/
183. RSA Key Exchange and Forward Secrecy - Cryptography Essentials - YouTube, accessed on April 21, 2025, https://www.youtube.com/watch?v=1w6SFzmln0Q
184. RSA Signatures - Practical Cryptography for Developers, accessed on April 21, 2025, https://cryptobook.nakov.com/digital-signatures/rsa-signatures
185. RSA and Digital Signatures | GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/rsa-and-digital-signatures/
186. Digital Signatures using RSA Public Key Cryptosystem Scheme - Research Trend, accessed on April 21, 2025, https://www.researchtrend.net/ijtas/pdf/7%20Digital%20Signatures%20using%20RSA%20Public%20Key%20Cryptosystem%20Scheme%20ARUN%20KUMAR%20SHARMA%201262.pdf
187. RSA Signatures - YouTube, accessed on April 21, 2025, https://www.youtube.com/watch?v=TeuKV5kHLyQ
188. RSA Signing is Not RSA Decryption - Computer Science Cornell, accessed on April 21, 2025, https://www.cs.cornell.edu/courses/cs5430/2015sp/notes/rsa_sign_vs_dec.php
189. How does RSA signature verification work? - Cryptography Stack Exchange, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/9896/how-does-rsa-signature-verification-work
190. Generate RSA Keys - Informatica Documentation, accessed on April 21, 2025,

https://docs.informatica.com/data-engineering/data-engineering-integration/h2l/1421-integrating-informatica--big-data-management-10-2-2-hf1-sp1/integrating-informatica--big-data-management-10-2-2-hf1-sp1-with/prepare-the-aws-environment/generate-rsa-keys.html
191. Generate RSA Key Pair - Auth0, accessed on April 21, 2025, https://auth0.com/docs/secure/application-credentials/generate-rsa-key-pair
192. Steps of Key Generation Using RSA Algorithm - Tutorialspoint, accessed on April 21, 2025, https://www.tutorialspoint.com/what-are-the-steps-of-key-generation-using-rsa-algorithm
193. RSA Keys Generation | Ktor Documentation, accessed on April 21, 2025, https://ktor.io/docs/rsa-keys-generation.html
194. How to Use ssh-keygen to Generate a New SSH Key? - SSH Communications Security, accessed on April 21, 2025, https://www.ssh.com/academy/ssh/keygen
195. RSA (explained step by step) - CrypTool, accessed on April 21, 2025, https://www.cryptool.org/en/cto/rsa-step-by-step/
196. RSA Encryption Decryption & Key Generator Tool Online - Devglan, accessed on April 21, 2025, https://www.devglan.com/online-tools/rsa-encryption-decryption
197. RSA Algorithm - How does it work? - I'll PROVE it with an Example! -- Cryptography - Practical TLS, accessed on April 21, 2025, https://www.youtube.com/watch?v=Pq8gNbvfaoM
198. What is RSA? How does an RSA work? - Encryption Consulting, accessed on April 21, 2025, https://www.encryptionconsulting.com/education-center/what-is-rsa/
199. What Is a Diffie-Hellman Key exchange? - NinjaOne, accessed on April 21, 2025, https://www.ninjaone.com/it-hub/endpoint-security/what-is-a-diffie-hellman-key-exchange/
200. Diffie–Hellman key exchange - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
201. How Diffie-Hellman Key Exchange Provides Encrypted Communications | UpGuard, accessed on April 21, 2025, https://www.upguard.com/blog/diffie-hellman
202. What is the Diffie–Hellman protocol? | Kaspersky IT Encyclopedia, accessed on April 21, 2025, https://encyclopedia.kaspersky.com/glossary/diffie-hellman-protocol-dh/
203. "Diffie-Hellman Key Exchange" in plain English, accessed on April 21, 2025, https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english
204. 16.2 Diffie Hellman key exchange, accessed on April 21, 2025, https://math-sites.uncg.edu/sites/pauli/112/HTML/secdiffiehellman.html
205. Implementation of Diffie-Hellman Algorithm - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/implementation-diffie-hellman-algorithm/

206. Cryptography: Diffie-Hellman key exchange explained intuitively using colors - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/programming/comments/7qq1bh/cryptography_diffiehellman_key_exchange_explained/
207. A simple guide to Diffie-Hellman Key Exchange including the what, the how and the why, accessed on April 21, 2025, https://crypto.stackexchange.com/questions/111116/a-simple-guide-to-diffie-hellman-key-exchange-including-the-what-the-how-and-th
208. What is the Diffie–Hellman (DH) Algorithm? | Security Encyclopedia - HYPR, accessed on April 21, 2025, https://www.hypr.com/security-encyclopedia/diffie-hellman-algorithim
209. What is Diffie Hellman Algorithm ? - Security Wiki - Secret Double Octopus, accessed on April 21, 2025, https://doubleoctopus.com/security-wiki/encryption-and-cryptography/diffie-hellman-algorithm/
210. Why use diffie hellman if I could just encrypt a key with the recipients public key? - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/cryptography/comments/q7njyt/why_use_diffie_hellman_if_i_could_just_encrypt_a/
211. Why is Diffie-Hellman presented as the solution for exchanging a key over an unsecure channel in security classes? : r/cryptography - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/cryptography/comments/artl8d/why_is_diffiehellman_presented_as_the_solution/
212. Guide to the Diffie-Hellman Key Exchange Algorithm & its Working | Simplilearn, accessed on April 21, 2025, https://www.simplilearn.com/tutorials/cryptography-tutorial/deffie-hellman-key-exchange
213. Diffie-Hellman key exchange, accessed on April 21, 2025, https://www.math.ucla.edu/~baker/40/handouts/rev_DH/node1.html
214. Create End-to-end Encryption Using the Diffie–Hellman Key Exchange | 8th Light, accessed on April 21, 2025, https://8thlight.com/insights/create-end-to-end-encryption-using-the-diffie-hellman-key-exchange
215. 2.3 Diffie–Hellman key exchange, accessed on April 21, 2025, https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf
216. Diffie-Hellman Key Exchange Algorithm - 1Kosmos, accessed on April 21, 2025, https://www.1kosmos.com/security-glossary/diffie-hellman-key-exchange-algorithm/
217. 10. Diffie-Hellman Key Exchange - Computer Security - CS 161, accessed on April 21, 2025, https://textbook.cs161.org/crypto/key-exchange.html
218. What is the current security status of Diffie-Hellman key exchange?, accessed on April 21, 2025, https://security.stackexchange.com/questions/112313/what-is-the-current-securit

y-status-of-diffie-hellman-key-exchange
219. Understanding and verifying security of Diffie-Hellman parameters - Red Hat, accessed on April 21, 2025, https://www.redhat.com/en/blog/understanding-and-verifying-security-diffie-hellman-parameters
220. Myths about Diffie Hellman Key Exchange algorithm : r/cryptography - Reddit, accessed on April 21, 2025, https://www.reddit.com/r/cryptography/comments/t58ohn/myths_about_diffie_hellman_key_exchange_algorithm/
221. www.techtarget.com, accessed on April 21, 2025, https://www.techtarget.com/searchsecurity/definition/nonrepudiation#:~:text=Nonrepudiation%20ensures%20that%20no%20party,its%20signature%20on%20a%20document.
222. What is Transport Layer Security (TLS)? - Cloudflare, accessed on April 21, 2025, https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/
223. What Are The Different Types Of Network Security? - PurpleSec, accessed on April 21, 2025, https://purplesec.us/learn/network-security-types/
224. What Are the Best Practices for Securing TCP/IP Networks Against Cyber Threats?, accessed on April 21, 2025, https://www.edgenext.com/what-are-the-best-practices-for-securing-tcp-ip-networks-against-cyber-threats/
225. What is IPSec? - IPSec Protocol Explained - AWS, accessed on April 21, 2025, https://aws.amazon.com/what-is/ipsec/
226. IPsec (Internet Protocol Security) VPN | NordLayer Learn, accessed on April 21, 2025, https://nordlayer.com/learn/vpn/ipsec/
227. What is IP Security (IPSec) - GeeksforGeeks, accessed on April 21, 2025, https://www.geeksforgeeks.org/ip-security-ipsec/
228. www.tutorchase.com, accessed on April 21, 2025, https://www.tutorchase.com/answers/a-level/computer-science/how-does-the-transmission-control-protocol--tcp--handle-data-integrity#:~:text=One%20of%20the%20key%20ways,it%20in%20the%20packet%20header.
229. How does the Transmission Control Protocol (TCP) handle data integrity? - TutorChase, accessed on April 21, 2025, https://www.tutorchase.com/answers/a-level/computer-science/how-does-the-transmission-control-protocol--tcp--handle-data-integrity
230. A Comprehensive Guide to TCP/IP - PubNub, accessed on April 21, 2025, https://www.pubnub.com/guides/tcp-ip/
231. How is data integrity maintained in network communication? - TutorChase, accessed on April 21, 2025, https://www.tutorchase.com/answers/a-level/computer-science/how-is-data-integrity-maintained-in-network-communication
232. Transmission Control Protocol - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Transmission_Control_Protocol
233. Elements of security in a TCP/IP network - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/en/i/7.4?topic=security-elements-in-tcpip-network

234. Elements of security in a TCP/IP network - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/en/i/7.4.0?topic=security-elements-in-tcpip-network
235. TCP/IP Security, accessed on April 21, 2025, https://sites.ualberta.ca/dept/chemeng/AIX-43/share/man/info/C/a_doc_lib/aixbman/commadmn/tcp_scurity.htm
236. TCP Authentication Option (TCP-AO) | Junos OS - Juniper Networks, accessed on April 21, 2025, https://www.juniper.net/documentation/us/en/software/junos/transport-ip/topics/topic-map/tcp-configure-ao-bgp-ldp.html
237. Authentication protocol - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Authentication_protocol
238. Authentication Protocols: Types and Uses - adaptive.live, accessed on April 21, 2025, https://adaptive.live/blog/authentication-protocols-types-and-uses
239. What Is IPsec? - Palo Alto Networks, accessed on April 21, 2025, https://www.paloaltonetworks.sg/cyberpedia/what-is-ipsec
240. What Are Network Security Services and How Can They Protect Your Small Business? - Brightline IT, accessed on April 21, 2025, https://brightlineit.com/what-are-network-security-services-and-how-can-they-protect-your-small-business/
241. Cyber Security Services in Computer Security & Network Security - Serveline, accessed on April 21, 2025, https://www.serveline.co.uk/post/security-services-in-computer-security
242. Encryption choices: rsa vs. aes explained - Prey, accessed on April 21, 2025, https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes
243. engineering.purdue.edu, accessed on April 21, 2025, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture10.pdf
244. Rivest–Shamir–Adleman | RSA Algorithm Explained | Simplilearn - YouTube, accessed on April 21, 2025, https://www.youtube.com/live/vf1z7GlG6Qo
245. How does RSA Cryptography work? - YouTube, accessed on April 21, 2025, https://www.youtube.com/watch?v=qph77bTKJTM
246. What is IPsec? | How IPsec VPNs work - Cloudflare, accessed on April 21, 2025, https://www.cloudflare.com/learning/network-layer/what-is-ipsec/
247. Network Security Services - Wikipedia, accessed on April 21, 2025, https://en.wikipedia.org/wiki/Network_Security_Services
248. Elements of security in a TCP/IP network - IBM, accessed on April 21, 2025, https://www.ibm.com/docs/ssw_ibm_i_73/ddp/rbal1elementsusetcp.htm
249. What is SSL/TLS Certificate? - AWS - Amazon.com, accessed on April 21, 2025, https://aws.amazon.com/what-is/ssl-certificate/
250. What is TLS/SSL and How It Works - Encryption Consulting, accessed on April 21, 2025, https://www.encryptionconsulting.com/education-center/what-is-tls-ssl/
251. What is SSL, TLS and HTTPS? - DigiCert, accessed on April 21, 2025, https://www.digicert.com/what-is-ssl-tls-and-https
252. Secure Your Website and Boost Trust with TLS/SSL Certificates - Entrust, accessed on April 21, 2025,

https://www.entrust.com/products/digital-certificates/tls-ssl
253. DigiCert: TLS/SSL Certificate Authority | Leader in Digital Trust, accessed on April 21, 2025, https://www.digicert.com/
254. Appendix A. Encryption Standards | Red Hat Product Documentation, accessed on April 21, 2025, https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/6/html/security_guide/chap-security_guide-encryption_standards
255. Just how secure is the TCP/IP protocol? - EBU tech, accessed on April 21, 2025, https://tech.ebu.ch/docs/events/networks05/presentations/ebu_networks05_leigh.pdf