

UNIT 7

Network Security

(5 Hours) — Computer Networking (CACS303)

As networks connect more devices and carry increasingly sensitive data, protecting that data from disclosure, alteration, and disruption becomes essential. Network security is the collection of policies, mechanisms, and technologies used to protect the confidentiality, integrity, and availability of data as it is stored and transmitted across a network. This unit introduces a general model for thinking about network security, the two major families of cryptographic techniques, the RSA public key algorithm, digital signatures, and the practical technologies used to secure real communications — IPSec, VPNs, firewalls, and wireless security.

7.1 A Model for Network Security

A useful general model for network security considers a message being sent from a sender to a receiver over an information channel, in the presence of an opponent — a party who may attempt to eavesdrop on, intercept, or alter the message. To defend against this opponent, two things are generally required: a security-related transformation applied to the message before it is sent (such as encryption, or adding a code that verifies the message's authenticity), and some secret information (a key) shared between the sender and receiver, but not known to the opponent. Often, a trusted third party is also involved — for example, to distribute the secret key to both parties securely, or to arbitrate disputes about the authenticity of a message.

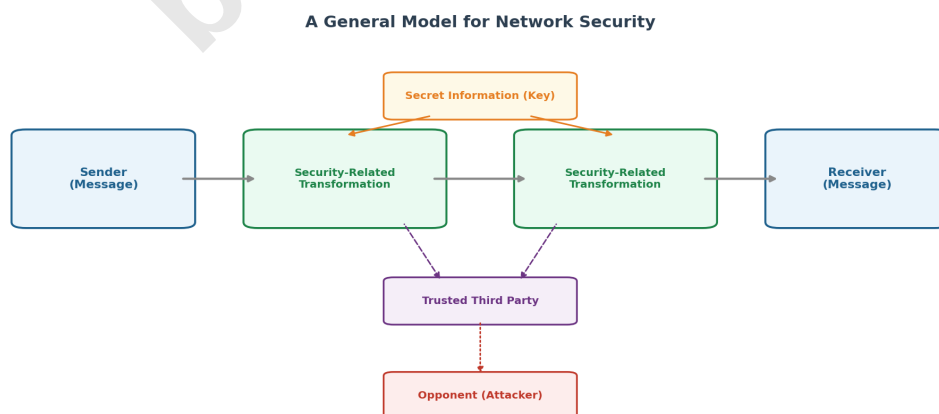


Figure 7.1: A general model for network security

This model highlights four essential tasks in designing a security service:

- Designing an algorithm for performing the security-related transformation, which should be strong enough that an opponent cannot defeat its purpose.

- Generating the secret information (keys) used with the algorithm.
- Developing methods to distribute and share the secret information securely between the two parties.
- Specifying a protocol that uses the security algorithm and the secret information to achieve a particular security service (such as confidentiality or authentication).

From this general model, we can identify the core goals — often summarized as the CIA triad plus authentication and non-repudiation:

Security Goal	Meaning
Confidentiality	Preventing unauthorized parties from reading the message content
Integrity	Ensuring the message is not altered, accidentally or maliciously, in transit
Availability	Ensuring authorized users can access systems and data when needed
Authentication	Verifying that a message (or user) genuinely originates from the claimed source
Non-repudiation	Preventing a sender from later denying that they sent a particular message

Key Takeaways — 7.1

- ✓ The security model involves a sender, receiver, opponent, a security transformation, and a shared secret.
- ✓ A trusted third party may help distribute keys or arbitrate disputes.
- ✓ Core goals: confidentiality, integrity, availability, authentication, and non-repudiation.

7.2 Principles of Cryptography: Symmetric Key and Public Key

Cryptography is the practice of transforming readable data (plaintext) into an unreadable form (ciphertext) using an algorithm and a key, such that only someone possessing the correct key can recover the original plaintext. The two fundamental approaches differ in how keys are used and shared.

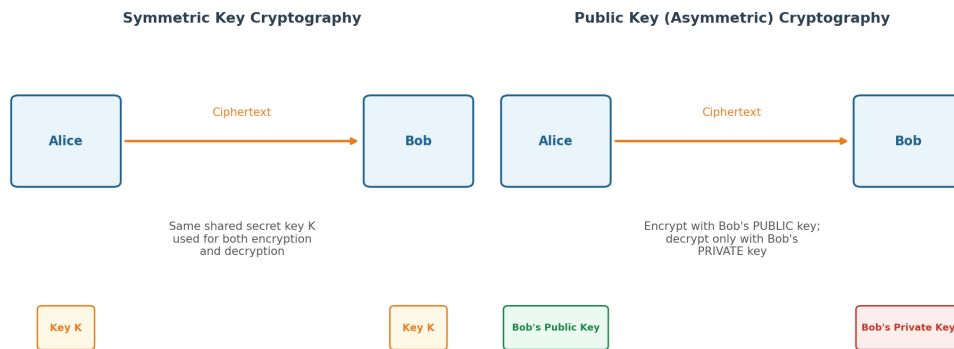


Figure 7.2: Symmetric key cryptography (single shared key) vs. public key cryptography (separate public/private key pair)

Symmetric Key Cryptography

In symmetric key (also called secret key or private key) cryptography, the same key is used for both encryption and decryption. Both the sender and receiver must possess this shared secret key in advance, and it must be exchanged through some secure channel before communication begins. Symmetric algorithms (such as AES and DES) are generally very fast and efficient for encrypting large volumes of data, but they face a significant challenge: securely distributing the shared key to all parties who need it, especially as the number of communicating parties grows.

Public Key (Asymmetric) Cryptography

In public key cryptography, each party has a pair of mathematically related keys: a public key, which can be freely shared with anyone, and a private key, which is kept secret. Data encrypted with a person's public key can only be decrypted with that same person's private key. This elegantly solves the key-distribution problem of symmetric cryptography — there is no need to secretly share a key in advance, since the public key can be published openly. The trade-off is that public key algorithms (such as RSA) are computationally much more expensive than symmetric algorithms, so in practice they are often used to securely exchange a symmetric session key, which then handles the bulk data encryption.

Aspect	Symmetric Key Cryptography	Public Key Cryptography
Keys used	One shared secret key	A public/private key pair per party
Speed	Fast — suited to bulk data encryption	Slower — computationally expensive
Key distribution	Must be exchanged securely in advance	Public key can be shared openly
Scalability	Harder to manage as parties increase	Scales more easily
Examples	AES, DES, 3DES	RSA, ECC, Diffie-Hellman

Note: In practice, most secure systems (like HTTPS) use a hybrid approach: public key cryptography to safely exchange a one-time symmetric session key, then symmetric encryption for the fast, ongoing encryption of the actual data.

Key Takeaways — 7.2

- ✓ Symmetric cryptography uses one shared key; fast but hard to distribute securely.
- ✓ Public key cryptography uses a public/private key pair; solves key distribution but is slower.
- ✓ Real systems typically combine both: public key to exchange a session key, symmetric for bulk data.

7.3 Public Key Algorithm — RSA

RSA (named after its inventors Rivest, Shamir, and Adleman) is the most widely used public key algorithm. Its security rests on the practical difficulty of factoring the product of two large prime numbers. RSA key generation, encryption, and decryption proceed as follows:

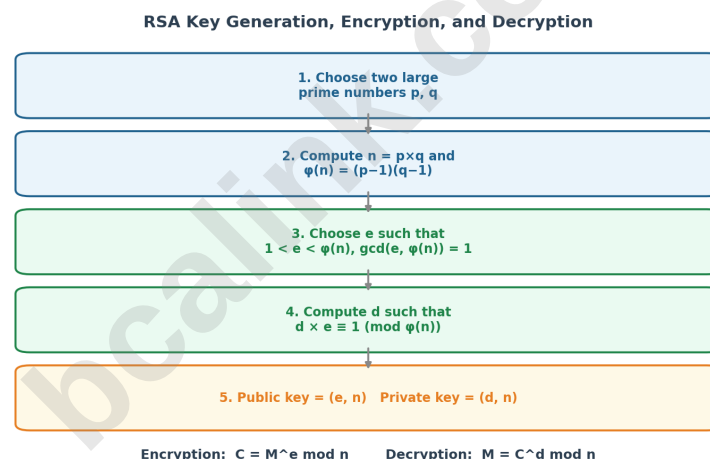


Figure 7.3: Steps of the RSA algorithm

Step	Description
1	Choose two large, distinct prime numbers p and q
2	Compute $n = p \times q$, and Euler's totient $\phi(n) = (p-1)(q-1)$
3	Choose a public exponent e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$
4	Compute the private exponent d such that $d \times e \equiv 1 \pmod{\phi(n)}$
5	Publish the public key (e, n) ; keep the private key (d, n) secret
6	Encrypt a message M as: $C = M^e \bmod n$
7	Decrypt the ciphertext C as: $M = C^d \bmod n$

Example 7.1 — RSA Key Generation and Encryption (small numbers)

Let $p = 7$ and $q = 11$. Generate an RSA key pair and use it to encrypt the message $M = 9$.

Solution

$$n = p \times q = 7 \times 11 = 77$$

$$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$$

Choose $e = 7$, since $\gcd(7, 60) = 1$ (7 and 60 share no common factors) and $1 < 7 < 60$.

Find d such that $d \times 7 \equiv 1 \pmod{60}$. Testing $d = 43$: $43 \times 7 = 301 = 5 \times 60 + 1$, so $d = 43$ works.

Public key = $(e, n) = (7, 77)$. Private key = $(d, n) = (43, 77)$.

Encryption: $C = M^e \bmod n = 9^7 \bmod 77 = 37$.

Decryption (check): $M = C^d \bmod n = 37^{43} \bmod 77 = 9$, recovering the original message.

Note: In real deployments, p and q are hundreds of digits long, making n far too large to factor with current computing power — this is what makes RSA secure in practice, even though the underlying arithmetic is the same as in this small example.

Key Takeaways — 7.3

- ✓ RSA security relies on the difficulty of factoring $n = p \times q$ for large primes.
- ✓ Public key (e, n) is used to encrypt; private key (d, n) is used to decrypt.
- ✓ Encryption: $C = M^e \bmod n$. Decryption: $M = C^d \bmod n$.

7.4 Digital Signature Algorithm

A digital signature is the electronic equivalent of a handwritten signature: it provides authentication (proof of who sent a message), integrity (proof the message was not altered), and non-repudiation (the sender cannot later deny having sent it). Digital signatures rely on public key cryptography, but used in the opposite direction from normal encryption — the sender signs using their own private key, and anyone can verify the signature using the sender's public key.

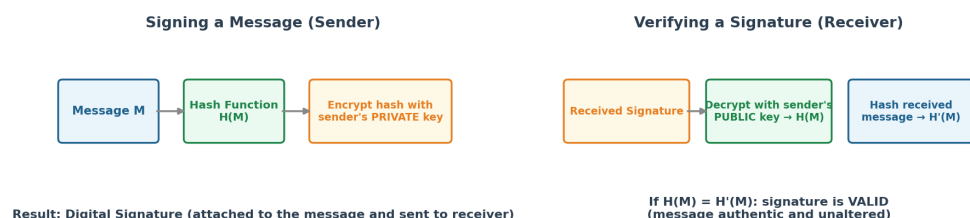


Figure 7.4: Digital signature process — signing with the sender's private key, verifying with the sender's public key

Signing Process

To sign a message, the sender first computes a fixed-size hash (a digital fingerprint) of the message using a cryptographic hash function, such as SHA-256. The sender then encrypts this hash using their own private key — the result is the digital signature, which is attached to the original message before it is sent.

Verification Process

Upon receiving the message and its attached signature, the receiver independently computes the hash of the received message, and separately decrypts the received signature using the sender's public key to recover the original hash the sender computed. If the two hash values match, the signature is valid: the message is confirmed to be authentic (it truly came from the claimed sender, since only that sender's private key could have produced a signature decryptable with their public key) and unaltered (any change to the message would change its hash and cause a mismatch).

Property	How the Digital Signature Provides It
Authentication	Only the sender's private key could have produced a signature decryptable by the sender's public key
Integrity	Any change to the message changes its hash, causing verification to fail
Non-repudiation	The sender cannot deny signing, since only they hold the private key used

Note: A digital signature does not by itself provide confidentiality — the message content is not hidden. If secrecy is also required, the message must additionally be encrypted (e.g. with the receiver's public key).

Key Takeaways — 7.4

- ✓ Digital signatures are created by hashing a message, then encrypting the hash with the sender's private key.
- ✓ Verification decrypts the signature with the sender's public key and compares hashes.
- ✓ Provides authentication, integrity, and non-repudiation — not confidentiality by itself.

7.5 Communication Security: IPSec, VPN, Firewalls, Wireless Security

IPSec (Internet Protocol Security)

IPSec is a suite of protocols that adds security services directly at the IP layer, so that any application using IP can benefit from protected communication without being individually modified. It provides confidentiality (via encryption), integrity, and authentication of IP packets, and can operate in two modes:

- Transport mode: Only the payload of the IP packet is encrypted/authenticated; the original IP header is left intact. Typically used for end-to-end communication between two hosts.
- Tunnel mode: The entire original IP packet (header and payload) is encrypted and encapsulated inside a new IP packet. Typically used between gateways (routers/firewalls) to protect traffic between two networks — this is the basis of most site-to-site VPNs.

VPN (Virtual Private Network)

A VPN extends a private network across a public network (typically the Internet), allowing remote users or remote sites to send and receive data as though their devices were directly connected to the private network. VPNs achieve this using tunneling protocols — often IPSec, but also alternatives like SSL/TLS-based VPNs — to encrypt and encapsulate traffic between the two endpoints.

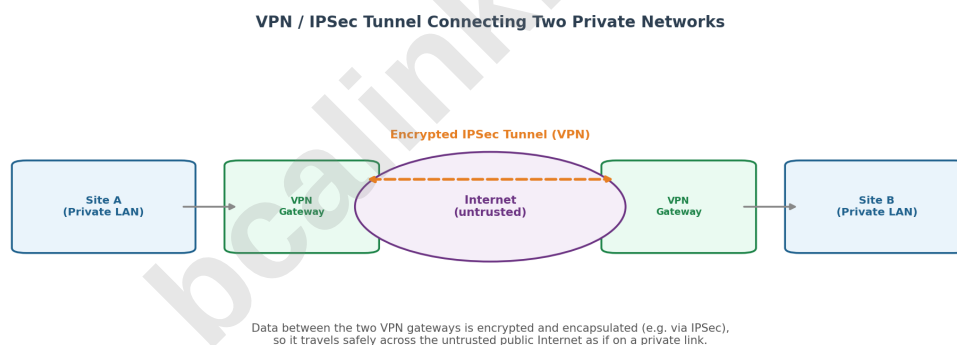
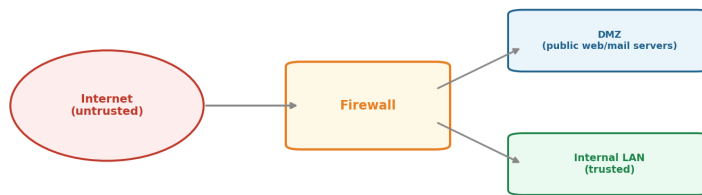


Figure 7.5: A site-to-site VPN using an encrypted IPSec tunnel over the public Internet

Firewalls

A firewall is a network security device (hardware, software, or both) that monitors and controls incoming and outgoing traffic based on a defined set of security rules, acting as a barrier between a trusted internal network and an untrusted external network such as the Internet.

Firewall Placement Between Untrusted and Trusted Networks



The firewall inspects and filters traffic between the untrusted Internet and the organization's networks, permitting only traffic that matches its security rules.

Figure 7.6: Firewall placement between untrusted and trusted networks, with a DMZ

Firewall Type	How It Works
Packet-filtering firewall	Examines individual packet headers (source/destination IP, port, protocol) against a rule set
Stateful inspection firewall	Tracks the state of active connections and allows only packets that fit an established, legitimate session
Application-level gateway (proxy)	Inspects traffic at the application layer, understanding specific protocols (e.g. HTTP, FTP) for finer control
Next-generation firewall (NGFW)	Combines traditional filtering with deep packet inspection, intrusion prevention, and application awareness

Note: Organizations often place public-facing servers (web, mail) in a DMZ (demilitarized zone) — a separate, more restricted network segment — so that even if a public server is compromised, the attacker still cannot directly reach the internal trusted LAN.

Wireless Security

Wireless networks broadcast signals over open air, making them inherently more exposed to eavesdropping and unauthorized access than wired networks, so encryption and authentication standards are essential. Wi-Fi security standards have evolved considerably:

Standard	Encryption	Notes
WEP (Wired Equivalent Privacy)	RC4 (weak, static keys)	Obsolete — easily broken; should not be used
WPA (Wi-Fi Protected Access)	TKIP (improved over WEP)	Interim fix for WEP's flaws; also now considered weak
WPA2	AES-CCMP (strong)	Long-standing standard; vulnerable to some attacks (e.g. KRACK) if unpatched
WPA3	AES with SAE (Simultaneous Authentication of Equals)	Current standard; stronger protection against offline password-guessing attacks

- SSID broadcasting control and MAC address filtering can add minor obstacles for casual intruders, though neither is a strong security measure on its own.
- Enterprise networks typically use WPA2/WPA3-Enterprise with 802.1X authentication against a central server (e.g. RADIUS), rather than a single shared password, giving each user their own credentials.

Key Takeaways — 7.5

- ✓ IPsec secures IP traffic directly, in transport mode (host-to-host) or tunnel mode (gateway-to-gateway, used by VPNs).
- ✓ VPNs extend a private network across the public Internet using encrypted tunnels.
- ✓ Firewalls filter traffic between trusted and untrusted networks; a DMZ isolates public-facing servers.
- ✓ Wireless security has progressed from broken WEP, through WPA/WPA2, to the current WPA3 standard.

— *End of Unit 7* —