

Cryptography and Network Security

Cryptography & Network Security – Structured Study Notes

1. Foundations

Concept	Definition	Goal
Cryptography	The science of securing information by transforming it into an unreadable form for unauthorized parties.	Confidentiality, integrity, authentication, non-repudiation
Network Security	The practice of protecting the integrity, confidentiality, and availability of data and resources as they travel across or reside in a network.	Prevent unauthorized access, detect attacks, ensure reliable service

2. Core Cryptographic Primitives

Primitive	Typical Use	Example Algorithms
Symmetric Encryption	Fast bulk data protection; both parties share a secret key.	AES, DES, 3DES, ChaCha20
Asymmetric Encryption (Public-Key)	Secure key exchange, digital signatures, encryption without prior shared secret.	RSA, ECC (Elliptic Curve), Diffie-Hellman (key agreement)
Hash Functions	Produce a fixed-size digest; used for integrity checking & password storage.	SHA-256, SHA-3, BLAKE2
Message Authentication Codes (MAC)	Verify data integrity & authenticity using a shared secret.	HMAC-SHA256, CMAC, Poly1305
Digital Signatures	Provide non-repudiation & authentication of origin.	RSA-PSS, ECDSA, EdDSA
Key Derivation Functions (KDF)	Stretch low-entropy secrets into cryptographically strong keys.	PBKDF2, HKDF, Argon2, scrypt

Cryptography and Network Security

3. Symmetric Encryption in Detail

Aspect	Details
Block Ciphers	Operate on fixed-size blocks (e.g., 128-bit). Modes of operation add security: CBC, CTR, GCM, OCB.
Stream Ciphers	Produce a keystream XORed with plaintext; useful for low-latency traffic. Examples: ChaCha20, Salsa20.
Key Management	Keys must be generated with high entropy, stored securely (HSMs, TPM), rotated regularly, and destroyed when obsolete.
Common Pitfalls	Reusing IVs/nonce, weak key derivation, ECB mode (reveals patterns).

4. Asymmetric Cryptography & Key Exchange

Topic	Key Points
RSA	Based on integer factorization. Key sizes ≥ 2048-bits for modern security.
Elliptic Curve Cryptography (ECC)	Security per bit is higher; 256-bit curve ≈ 3072-bit RSA. Popular curves: secp256r1, Curve25519, Ed25519.
Diffie-Hellman (DH)	Allows two parties to derive a shared secret over an insecure channel. Use with authenticated groups (e.g., ECDH).
Hybrid Encryption	Combine asymmetric (to exchange a symmetric session key) with symmetric encryption for data payload – the standard model for TLS, PGP, S/MIME.
Certificate Authorities (CAs)	Issue X.509 certificates binding public keys to identities. Revocation mechanisms: CRL, OCSP.

5. Cryptographic Hashes & Integrity

Property	Explanation
Pre-image resistance	Hard to find any input that hashes to a given output.
Second-pre-image resistance	Hard to find