Edversity.

CYBERSECURITY SPECIALIZATION PROGRAM WEEK 3 - DAY 2

Instructor: Muddassir Shafique

TA: Suleiman Taj

What We'll Learn Today

- Modern Cryptography & Real-World Applications
- Symmetric (AES) and Asymmetric (RSA, Public/Private keys)
- Hashing (SHA-256), digital signatures
- Where cryptography is used (banking, passwords, messaging apps)
- Practical

Modern Cryptography

Modern cryptography is the science and practice of securing digital information and communications using mathematics, algorithms, and computing power. Unlike classical methods, modern cryptography is built to withstand advanced attacks and is the foundation of security in the digital world.

It is based on principles like:

Confidentiality – Keeping information private.

Integrity – Ensuring data hasn't been tampered with.

Authentication – Verifying identities.

Non-repudiation – Preventing denial of actions or messages.

Modern cryptography is the backbone of cybersecurity in the digital age — securing your emails, passwords, bank accounts, private messages, cloud files, and even your cryptocurrency wallet.

Real-World Applications of Modern Cryptography

1. Secure Communication (Messaging & Email)

- Apps like WhatsApp, Signal, and Telegram use end-to-end encryption so only the sender and recipient can read messages.
- PGP (Pretty Good Privacy) secures email communication.

2. Online Banking & Payments

- Cryptography protects sensitive data like credit card numbers, PINs, and transaction details.
- SSL/TLS protocols ensure your connection to bank websites is encrypted.

3. Secure Websites (HTTPS)

- Websites with HTTPS use SSL/TLS certificates to encrypt data between your browser and the website.
- Protects against man-in-the-middle attacks.

Real-World Applications of Modern Cryptography

4. Data Protection & Storage

- Full-disk encryption tools (e.g., BitLocker, VeraCrypt) encrypt data at rest.
- Cloud services (e.g., Google Drive, Dropbox) use encryption to protect stored files.

5. Digital Signatures & Certificates

- Used to verify the sender's identity and ensure data integrity.
- Digital certificates (e.g., from DigiCert, Let's Encrypt) secure software, websites, and documents (like PDFs).

6. Authentication Systems

- Passwords, OTPs, biometrics, and 2FA rely on cryptographic functions.
- Authentication tokens (e.g., Google Authenticator) use time-based cryptography.

Real-World Applications of Modern Cryptography

7. Blockchain & Cryptocurrencies

- Blockchain ensures immutability and trustless verification.
- Bitcoin, Ethereum use cryptographic hashes and digital signatures for secure, verifiable transactions.

8. Virtual Private Networks (VPNs)

- VPNs encrypt internet traffic, hiding your activity from ISPs and hackers.
- Uses modern encryption protocols (e.g., IPSec, OpenVPN, WireGuard).

9. Government & Military

- Cryptography secures classified communications, surveillance, and national security systems.
- Includes both encryption and secure key exchange mechanisms.

Types of Modern Cryptography

- Symmetric algorithms (e.g., AES)
- Asymmetric algorithms (e.g., RSA, ECC)
- Hash functions (e.g., SHA-256)
- Digital signatures, certificates, and secure protocols (e.g., SSL/TLS, HTTPS)

Types of Modern Cryptography

Symmetric algorithms (e.g., AES)

Definition:

- A symmetric algorithm is a type of encryption where the same key is used for both encryption and decryption of data.
- One key to lock, the same key to unlock.

Purpose:

- To ensure confidentiality of information during storage or transmission, especially where both sender and receiver can securely share a single secret key.
- Used to protect data quickly and efficiently.
- Ideal for encrypting large volumes of data.

Types of Modern Cryptography

Popular Symmetric Algorithms

Algorithm	Description
AES (Advanced Encryption Standard)	Industry standard; very secure and fast
DES (Data Encryption Standard)	Older; replaced by AES due to weak security
3DES (Triple DES)	Improved version of DES (encrypt-decrypt-encrypt)
Blowfish / Twofish	Fast and flexible encryption for software

Types of Modern Cryptography

What is AES (Advanced Encryption Standard)?

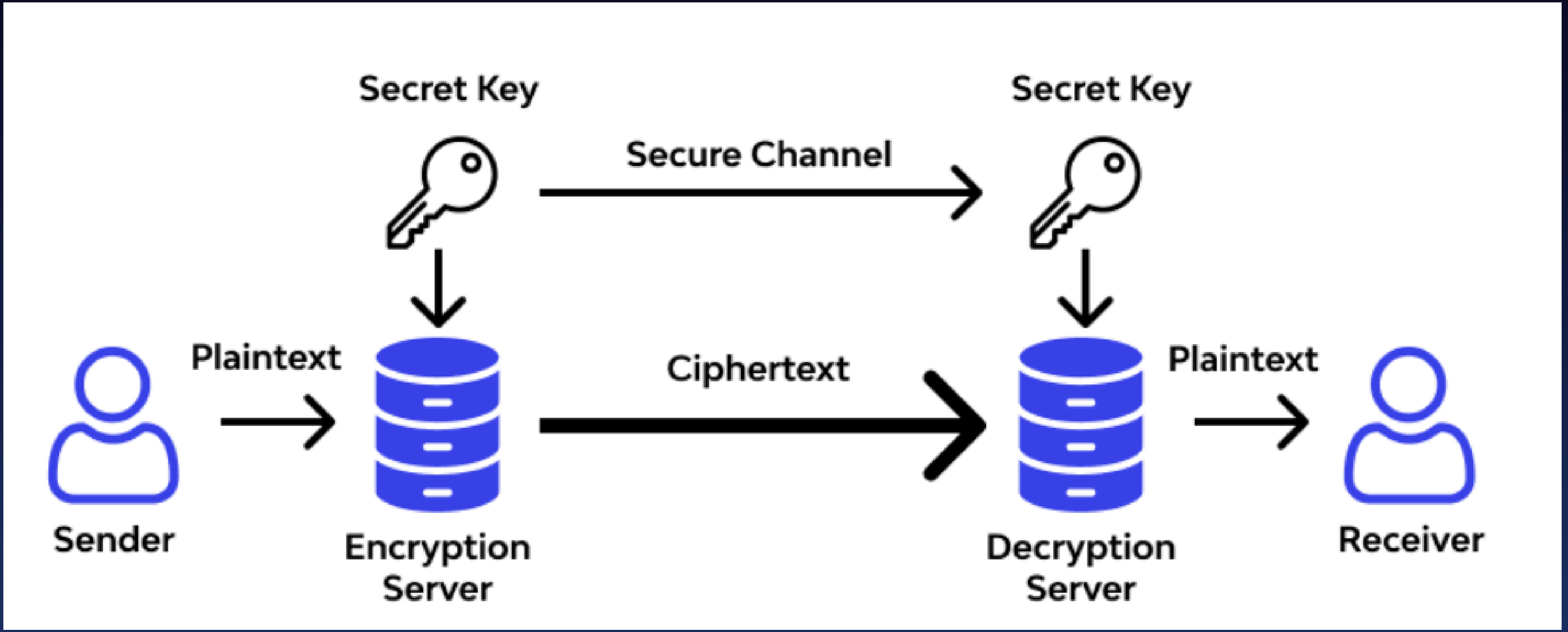
AES (Advanced Encryption Standard) is a symmetric block cipher used worldwide to secure data. It's the de facto industry standard for encrypting sensitive information due to its speed, security, and efficiency.

Types of Modern Cryptography

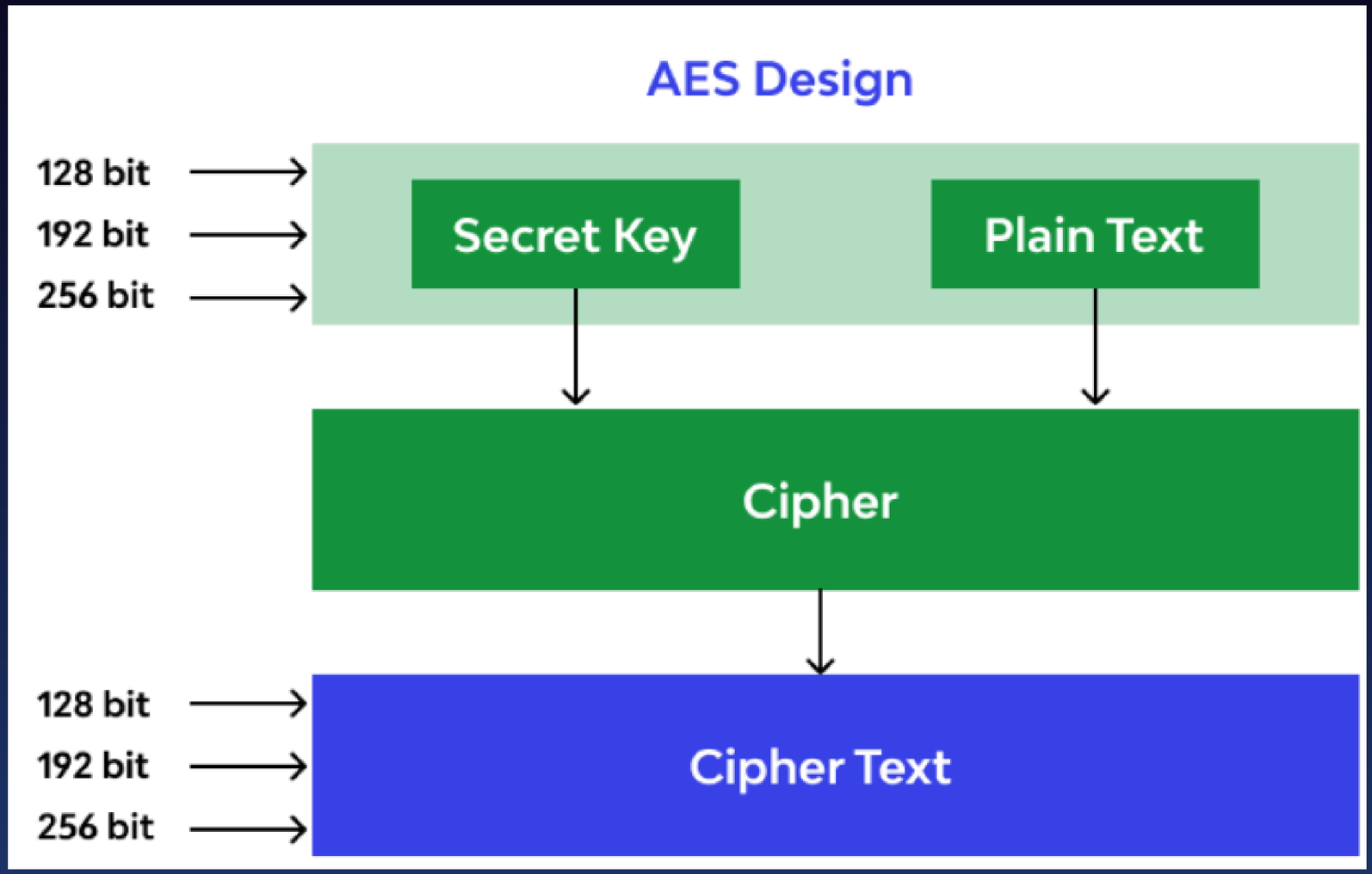
AES KEY FEATURES

Feature	Description
Type	Symmetric encryption (same key for encrypt/decrypt)
Block Size	128 bits
Key Sizes	128, 192, or 256 bits
Rounds	10 (128-bit), 12 (192-bit), 14 (256-bit)
Standardized by	NIST (National Institute of Standards and Technology)
Algorithm Family	Substitution–Permutation Network (SPN)

Types of Modern Cryptography



Types of Modern Cryptography



Types of Modern Cryptography

How AES Works (Simplified)

Key Expansion

- The key is expanded into multiple round keys using a key schedule algorithm.

Initial Round

- AddRoundKey: Input block is combined with the first round key.

Types of Modern Cryptography

Main Rounds (10/12/14 times)

- **SubBytes:** Each byte is substituted using an S-box (non-linear substitution).
- **ShiftRows:** Rows of the state are shifted.
- **MixColumns:** Columns are mixed using a mathematical operation.
- AddRoundKey: Round key is added to the state.

Types of Modern Cryptography

AddRoundKey: Round key is added to the state.

Final Round: Like main rounds, but without MixColumns.

Types of Modern Cryptography

AES in Real Life

Use Case	Example
Banking & Payments	Encrypting card transactions
Secure Messaging	WhatsApp, Signal
File/Storage Encryption	BitLocker, VeraCrypt
VPNs	Encrypting internet traffic
Cloud Data Security	Amazon S3, Google Cloud

Types of Modern Cryptography

Online Tools to Practice AES

Tool	URL	Features
CyberChef (by GCHQ)	https://gchq.github.io/CyberChef	Drag & drop AES encryption/decryption
Online-Toolz AES	https://www.online-toolz.com/tools/text-encryption-decryption.php	Simple AES in ECB/CBC modes
Devglan AES Tool	https://www.devglan.com/online-tools/aes-encryption-decryption	Key, IV input, AES-128/192/256
Cryptii	https://cryptii.com	Visual transformations, including AES

Asymmetric Algorithms

Definition:

An asymmetric algorithm is a type of encryption that uses two different but mathematically linked keys:

- A public key (shared openly)
- A private key (kept secret)

What one key encrypts, only the other can decrypt — and vice versa.

Asymmetric Algorithms

Purpose:

- To solve the key distribution problem found in symmetric encryption by allowing secure communication without sharing secret keys in advance.
- Enables confidentiality, authentication, and digital signatures in modern security systems.

Asymmetric Algorithms

How It Works (Method):

For Encryption (Confidentiality):

1. Sender encrypts the message using the recipient's public key.
2. Only the recipient's private key can decrypt it.

Asymmetric Algorithms

For Digital Signatures (Authentication & Integrity):

- Sender signs data using their private key.
- Anyone can verify the signature using the sender's public key.
- Public key = lock
- Private key = unique unlock

Types of Modern Cryptography

Popular Asymmetric Algorithms

Algorithm	Use Case
RSA	Widely used for secure web traffic, email, digital signatures
ECC (Elliptic Curve Cryptography)	Strong security with shorter keys (used in modern systems)
DSA (Digital Signature Algorithm)	Used specifically for digital signing
ElGamal	Encryption and key exchange

Hash Functions

Definition:

- A hash function is a mathematical algorithm that takes an input (any size) and returns a fixed-size string of characters — typically called a hash value or digest.
- It's a one-way function: easy to compute the hash, but impossible to reverse back to the original data.

Purpose:

- To verify data integrity by detecting any changes to the original data.
- Widely used in password storage, digital signatures, blockchain, and file verification.

Types of Modern Cryptography

How It Works (Method):

- Input any message or file (e.g., Hello World).
- Apply a hash function (e.g., SHA-256).
- Output: a fixed-size string (e.g., 256-bit digest).

Popular Hash Algorithms:

Algorithm	Output Size	Status
MD5	128-bit	Weak / Broken ❌
SHA-1	160-bit	Weak / Collisions found ❌
SHA-256	256-bit	Secure ✅
SHA-3	Variable	New and secure ✅
Bcrypt, Argon2	Variable	Designed for secure password hashing ✅

Digital Signature

Definition

- A digital signature is a cryptographic technique used to validate the authenticity and integrity of digital messages or documents.** It proves:
- The message was sent by the claimed sender (authenticity).
- The message was not changed during transmission (integrity).
- It’s the digital equivalent of a handwritten signature — but much more secure.

Digital Signature

Purpose of Digital Signatures:

- To verify identity (authentication)
- To ensure message integrity
- To prevent tampering
- To provide non-repudiation (sender can’t deny they sent it)

Used in:

- Email security
- Software signing
- Legal e-documents
- Blockchain & cryptocurrencies
- SSL/TLS certificates

Digital Signature

How Digital Signatures Work:

- It uses Asymmetric Cryptography:
- Sender creates a hash (digest) of the message.
- The sender encrypts the hash using their private key.
- This encrypted hash is the digital signature.

Receiver receives:

- the original message
- the digital signature

Digital Signature

Receiver:

- Hashes the received message using the same hash algorithm.
- Decrypts the signature using the sender's public key to get the original hash.
- Compares both hashes:
- If they match → message is authentic and unchanged.
- If not → the message was tampered with or not from the real sender.

Comparison

Feature / Aspect	🔒 Symmetric Algorithms	🔐 Asymmetric Algorithms	🧮 Hash Functions	✍️ Digital Signatures
Basic Definition	Encryption using **one shared secret key**	Encryption using **public/private key pair**	One-way function converting input to fixed-size digest	Sign and verify data using **private/public keys**
Keys Involved	1 key (same for encryption & decryption)	2 keys (public and private)	No keys	2 keys (sign with private, verify with public)
Main Purpose	Fast, bulk **data encryption/decryption**	**Secure communication** & key exchange	**Verify data integrity**	**Authenticate sender** and verify data integrity
Direction	Reversible	Reversible	One-way (irreversible)	One-way + verifiable
Speed	🔼 Fast	🔽 Slower	🔼 Fast	🔽 Slower (due to hashing + encryption)
Use Case Examples	File encryption, VPN, secure storage	SSL/TLS, secure email, key exchange	Passwords, blockchain, file integrity	E-signatures, legal docs, software verification

Comparison

Feature / Aspect	🔒 Symmetric Algorithms	🔐 Asymmetric Algorithms	🧮 Hash Functions	✍️ Digital Signatures
Key Management	Difficult at scale (everyone needs same key)	Easier (only public keys shared openly)	Not required	Requires PKI for key & identity management
Scalability	Poor (many users = many keys)	Good (1 key pair per user)	Excellent	Moderate (needs trust infrastructure)
Security Risk	If key is leaked, all messages are compromised	If private key is exposed, security is lost	Susceptible to collision (in weak hashes)	If private key is stolen, signatures can be forged
Real Examples	AES, DES, RC4	RSA, ECC, ElGamal	SHA-256, SHA-3, Bcrypt	RSA, DSA, ECDSA

What Cryptography is Used

1. Banking & Financial Services

- **Online Banking:** Encrypts transactions and login details (SSL/TLS).
- **ATMs:** Use symmetric encryption to communicate securely with the bank server.
- **Payment Cards:** EMV chips use cryptographic protocols.
- **Digital Signatures:** Used to authorize large or corporate fund transfers.

2. Password Protection

- **Hash Functions:** Passwords are stored as hashes, not plaintext.
- **Salted Hashing:** Adds randomness to hashes for more protection.
- **Multi-Factor Authentication (MFA):** Often involves cryptographic keys.

What Cryptography is Used

3. Messaging Apps

- **End-to-End Encryption (E2EE):** Only sender and receiver can read the message.
- **Apps like:**
- **WhatsApp –** Uses the Signal protocol (asymmetric + symmetric).
- **Signal –** Industry leader in secure messaging.
- **iMessage, Telegram (secret chat) –** Also use strong cryptography.

4. Web Security

- **HTTPS (SSL/TLS):** Encrypts data between browser and server.
- **SSL Certificates:** Use asymmetric cryptography and digital signatures.
- **Secure Cookies & Sessions:** Cryptographic tokens are used to identify users securely.

Types of Modern Cryptography

5. File & Data Protection

- **Full Disk Encryption:** Tools like BitLocker, VeraCrypt, FileVault.
- **Cloud Storage:** Services like Google Drive and Dropbox use encryption to protect stored and transmitted data.
- **Ransomware (misuse):** Cybercriminals use strong encryption to lock your data.

6. Emails & Digital Documents

- **PGP/GPG:** For encrypting emails.
- **S/MIME:** For email digital signatures and encryption.
- **PDF Signatures:** Legal digital documents are signed using cryptography.

Types of Modern Cryptography

7. Healthcare & Government

- **Electronic Health Records (EHR):** Encrypted for patient privacy (HIPAA compliance).
- **e-Voting systems:** Use encryption and digital signatures to protect vote confidentiality.
- **Military & Intelligence:** Use highly secure, custom-built cryptosystems.

8. Cryptocurrencies & Blockchain

- **Bitcoin, Ethereum:** Use asymmetric cryptography for transactions.
- **Hash functions:** Power blockchain security and proof-of-work algorithms.
- **Wallets:** Protect user assets using private/public key pairs.

Types of Modern Cryptography

9. Wireless & Network Security

- **Wi-Fi Encryption:** WPA2, WPA3 standards use AES encryption.
- **VPNs:** Use encryption to secure entire internet traffic.
- **Firewalls and Intrusion Detection Systems:** use cryptographic validation.

10. Identity & Access Management

- **Digital Certificates:** Validate user identity via trusted certificate authorities (CAs).
- **Smart Cards & Biometrics:** Store cryptographic data and validate access securely.
- **OAuth & JWT:** Use cryptographically signed tokens for web authentication.

Practical

Hashcat – Password Hash Cracker (also shows encryption/hashing types)

Supports:

- MD5, SHA1, SHA256, bcrypt, PBKDF2
- WPA/WPA2 handshake cracking
- Encrypted document brute-forcing
- hashcat -m 0 -a 0 hashes.txt wordlist.txt
- -m 0 → Hash type: MD5
- -a 0 → Attack mode: Dictionary attack
- hashes.txt → File containing one or more hashes
- /usr/share/wordlists/rockyou.txt → Wordlist with 14+ million common passwords
- echo -n "password123" | md5sum
-

OpenSSL – Swiss Army Tool for Encryption

Supports:

- **AES-128/192/256**
- **DES, 3DES, Blowfish**
- **RSA public-private key encryption**
- **Certificate generation**

OpenSSL – Swiss Army Tool for Encryption

Encrypt

openssl enc -aes-256-cbc -pbkdf2 -salt -in secret.txt -out secret.enc

-d

Decrypt mode

-aes-256-cbc

Use AES encryption in CBC mode

-pbkdf2

Use modern, secure key derivation

-in secret.enc

Encrypted input file

-out decrypted.txt

Decrypted output file

OpenSSL – Swiss Army Tool for Encryption

Decrypt

openssl enc -d -aes-256-cbc -in secret.enc -out secret.txt

Cryptool (cttool) – Classical & Modern Cipher CLI

Supports:

- Caesar, Vigenère, Affine, Substitution
- RSA, DES, AES
- Frequency analysis, brute-force
- sudo apt install cttool
- cttool caesar -e -s 5
- cttool vigenere -e -k MYKEY
- https://www.cryptool.org/en/cto/

GPG (GNU Privacy Guard) – Industry-Standard File Encryption

Supports:

RSA (asymmetric)

AES (symmetric)

Can encrypt files and verify signatures

Encrypt with password

gpg -c file.txt

Decrypt

gpg file.txt.gpg

Practical-Encryption

Cyber Chef

firefox https://gchq.github.io/CyberChef/

Supports:

- Caesar Cipher
- Vigenère
- AES / Blowfish / RC4
- XOR / Base64 / URL / JWT
- Hashing: SHA, MD5, bcrypt, etc.

How to encrypt and decrypt images

https://georgeom.net/StegOnline/upload

steghide embed -cf image.jpg -ef secret.txt

steghide extract -sf image.jpg

sudo apt install imagemagick

convert 1234.png 1234.jpg

https://georgeom.net/StegOnline/upload

steghide embed -cf image.jpg -ef secret.txt

steghide extract -sf image.jpg

sudo apt install imagemagick

convert 1234.png 1234.jpg

What We Learned Today

- Modern Cryptography & Real-World Applications
- Symmetric (AES) and Asymmetric (RSA, Public/Private keys)
- Hashing (SHA-256), digital signatures
- Where cryptography is used (banking, passwords, messaging apps)
- Practical