Cryptography Algorithms

DES (Data Encryption Standard)

Explanation: DES is a symmetric-key block cipher that was once the federal standard for data encryption. It uses a 56-bit key to encrypt 64-bit blocks of data.

Key features:

- Uses a Feistel network structure with 16 rounds
- 56-bit key (technically 64 bits, but 8 are parity bits)
- Now considered insecure due to short key length
- Vulnerable to brute force attacks

Example: If you want to encrypt the message "HELLO" with DES, each character would be converted to binary, divided into 64-bit blocks, and run through the 16-round encryption process with the secret key.

AES (Advanced Encryption Standard)

Explanation: AES replaced DES as the encryption standard. It's a symmetric block cipher that processes data in 128-bit blocks and supports key lengths of 128, 192, or 256 bits.

Key features:

- Based on substitution-permutation network
- Faster than DES in both hardware and software
- Highly resistant to various attacks
- Currently the most widely used symmetric encryption algorithm

Example: When you access an HTTPS website, AES is often used to encrypt the data transmitted between your browser and the server, typically using AES-256 (256-bit key).

RSA Algorithm

Explanation: RSA is an asymmetric encryption algorithm that uses a pair of keys: public key for encryption and private key for decryption. Its security is based on the difficulty of factoring large prime numbers.

Key features:

- Named after creators Rivest, Shamir, and Adleman
- Commonly used for secure data transmission
- Key lengths typically 2048 or 4096 bits
- Computationally intensive compared to symmetric algorithms

Example:

1. Alice generates public key (n,e) and private key (n,d)
2. Alice shares her public key with Bob
3. Bob encrypts message M: C = M^e mod n

4. Alice decrypts with private key: M = C^d mod n

Diffie-Hellman Key Exchange Algorithm

Explanation: Diffie-Hellman allows two parties to establish a shared secret key over an insecure channel without previously sharing any secrets.

Key features:

- First practical method for public key exchange
- Based on discrete logarithm problem
- Doesn't provide authentication by itself
- Vulnerable to man-in-the-middle attacks without additional authentication

Example:

1. Alice and Bob agree on public values: a prime number p and base g
2. Alice chooses secret a, calculates A = g^a mod p, sends A to Bob
3. Bob chooses secret b, calculates B = g^b mod p, sends B to Alice
4. Alice computes shared key: K = B^a mod p
5. Bob computes same key: K = A^b mod p
6. Both now have identical key K = g^(ab) mod p

Stream & Block Cipher Techniques

Block Ciphers:

- Process fixed-size blocks of data (e.g., 128 bits in AES)
- Same input block always produces the same output block with the same key
- Examples: DES, AES, Blowfish
- Different modes of operation include:
    - ECB (Electronic Codebook): simplest but least secure
    - CBC (Cipher Block Chaining): each block XORed with previous ciphertext
    - CTR (Counter): turns block cipher into stream cipher

Stream Ciphers:

- Process data one bit or byte at a time
- Uses a keystream generator to create a pseudorandom stream
- XOR the keystream with plaintext
- Examples: RC4, ChaCha20
- Advantage: faster, no padding required
- Weakness: reusing keystream is catastrophically insecure

Example: When encrypting a file with a block cipher like AES in CBC mode, if the file size isn't a multiple of the block size, padding is added to make it fit exactly.

Digital Signature

Explanation: Digital signatures provide authentication, non-repudiation, and integrity verification. They're created by encrypting a hash of the message with the sender's private key.

Key features:

- Verifiable by anyone with the signer's public key
- Cannot be forged without the private key
- Provides proof of document origin and integrity
- Often used with document hashing

Example:

1. Alice wants to sign a document
2. She creates a hash of the document
3. Alice encrypts the hash with her private key (the signature)
4. She sends both the document and signature to Bob
5. Bob hashes the received document
6. Bob decrypts the signature using Alice's public key
7. If the decrypted hash matches Bob's calculated hash, the signature is valid

Digital Certificates

Explanation: Digital certificates are electronic documents that bind a public key to an entity (person, organization, device). They're issued by Certificate Authorities (CAs) and help establish trust in online communications.

Key components:

- Subject's identity information
- Subject's public key
- Certificate issuance and expiration dates
- Certificate Authority's digital signature
- Certificate version, serial number

Example: When you visit an HTTPS website, your browser verifies the website's digital certificate to ensure you're connected to the legitimate server and not an impostor.

Hashing Functions

MD5 (Message Digest 5):

- Produces a 128-bit hash value
- Now considered cryptographically broken
- Still used for file integrity checking (not for security)

SHA (Secure Hash Algorithm):

- SHA-1: 160-bit output (deprecated)

- SHA-2 family: includes SHA-256, SHA-384, SHA-512
- SHA-3: newest standard, different internal structure
- Used for digital signatures, password storage, data integrity

Key features of good hash functions:

- Deterministic: same input always yields same output
- Fast to compute
- Infeasible to derive original message from hash
- Small changes to input cause large changes in output
- Collision-resistant: difficult to find two inputs with same hash

Example: Password storage in databases often uses salted hashes. If your password is "Password123", the system might store:

```
Username: user123
Salt: r4nd0m5tr1ng
Hash: SHA256("Password123r4nd0m5tr1ng") = a3d8e7f...
```

PKI (Public Key Infrastructure)

Explanation: PKI is a framework for managing digital certificates and public key encryption, enabling secure communications through trust relationships.

Key components:

- Certificate Authority (CA): issues and verifies certificates
- Registration Authority (RA): verifies user identities
- Certificate Repository: stores and distributes certificates
- Certificate Revocation List (CRL): lists invalid certificates

Example: When you establish an HTTPS connection to your bank's website, PKI provides:

1. Authentication: Verifies you're connected to the actual bank website
2. Confidentiality: Encrypts data between you and the bank
3. Integrity: Ensures data isn't tampered with in transit

Network Security

SNORT

Explanation: SNORT is an open-source network intrusion detection and prevention system (IDS/IPS) that performs real-time traffic analysis and packet logging.

Key features:

- Protocol analysis
- Content matching/searching
- Detect various attacks: buffer overflows, stealth port scans, CGI attacks
- Rule-based detection engine

- Can operate in three modes: sniffer, packet logger, or NIDS

Example: A SNORT rule to detect potential SSH brute force attempts:

```
alert tcp any any -> $HOME_NET 22 (msg:"Potential SSH brute force attempt";
flow:to_server; threshold:type threshold, track by_src, count 5, seconds 60;
classtype:attempted-admin; sid:1000001; rev:1;)
```

Access Control List (ACL)

Explanation: ACLs specify which users or system processes are granted access to objects, and what operations are allowed on given objects.

Types:

- Standard ACLs: Filter based on source IP address only
- Extended ACLs: Filter based on source/destination IP, protocols, ports
- Dynamic ACLs: Require authentication before permitting access
- Reflexive ACLs: Filter based on previous outbound traffic

Example: A router ACL to allow HTTP and HTTPS traffic to a web server:

```
access-list 101 permit tcp any host 192.168.1.100 eq 80
access-list 101 permit tcp any host 192.168.1.100 eq 443
access-list 101 deny ip any any
```

NAT & PAT

NAT (Network Address Translation):

- Translates private IP addresses to public IP addresses
- Helps conserve IPv4 address space
- Provides a layer of security by hiding internal network structure
- Types: Static NAT, Dynamic NAT, and PAT

PAT (Port Address Translation):

- A form of dynamic NAT that maps multiple private IP addresses to a single public IP
- Uses different port numbers to distinguish between translations
- Also called NAT Overload
- Most common form of NAT in home routers

Example:

1. Your computer (192.168.1.5) requests a webpage
2. Your router (public IP: 203.0.113.5) receives the request
3. Router changes the source IP from 192.168.1.5 to 203.0.113.5 and assigns a unique source port
4. Router maintains a translation table to keep track of connections
5. When responses return, router forwards them to the correct internal device

Wireless Networks

Wireless Network Standards & Types

Ad Hoc Network:

- Devices connect directly to each other without an access point
- Decentralized network structure
- Simple to set up but limited in scalability
- Useful for temporary connections between devices

Infrastructure Network:

- Devices connect through a central access point
- More scalable and manageable
- Provides better coverage and reliability
- Standard configuration for most wireless networks

Bluetooth

Explanation: Bluetooth is a short-range wireless technology standard for exchanging data between fixed and mobile devices over short distances.

Key features:

- Operates in 2.4 GHz ISM band
- Range: typically 10m (Class 2) to 100m (Class 1)
- Data rates: from 1 Mbps (Basic Rate) to 50 Mbps (Bluetooth 5)
- Uses frequency-hopping spread spectrum for security
- Security: pairing, encryption, authentication

Example: When you connect wireless headphones to your smartphone, they establish a Bluetooth connection using a pairing process where both devices exchange and store link keys.

WiFi

Explanation: WiFi is a family of wireless network protocols based on the IEEE 802.11 standards, commonly used for local area networking and Internet access.

Key standards:

- 802.11a: 5 GHz, up to 54 Mbps
- 802.11b: 2.4 GHz, up to 11 Mbps
- 802.11g: 2.4 GHz, up to 54 Mbps
- 802.11n (WiFi 4): 2.4/5 GHz, up to 600 Mbps
- 802.11ac (WiFi 5): 5 GHz, up to 3.5 Gbps
- 802.11ax (WiFi 6): 2.4/5/6 GHz, improved efficiency

Security protocols:

- WEP: Obsolete and insecure
- WPA: Improved security over WEP
- WPA2: Current standard with AES encryption
- WPA3: Latest standard with stronger protection

Example: A home WiFi network typically uses an infrastructure mode where multiple devices connect to a central router/access point operating on a specific channel within the 2.4 GHz or 5 GHz band.

WiMAX

Explanation: WiMAX (Worldwide Interoperability for Microwave Access) is a wireless broadband communication standard designed for longer-range connectivity.

Key features:

- Based on IEEE 802.16 standards
- Range: up to 50 km
- Data rates: up to 70 Mbps
- Can provide "last mile" wireless broadband access
- Can operate in licensed or unlicensed bands (2.3, 2.5, 3.5 GHz)
- Supports both line-of-sight and non-line-of-sight connectivity

Example: In rural areas where laying fiber or cable is expensive, WiMAX can provide broadband connectivity from a central tower to multiple homes and businesses within a large radius.

Is there any specific topic from this list that you'd like me to explain in more detail for your viva exam preparation?