Mathematics in Information Security

UNIT 2

Introduction to Cryptography

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries.

- Plaintext: The original, readable message or data.
- Ciphertext: The transformed, unreadable version of the plaintext.
- Key: A piece of information that determines the output of a cryptographic algorithm. Keys are essential for both encryption and decryption.

Introduction to Cryptography

Types of Cryptography:

There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:

1. Symmetric-key cryptography: This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.

2. Asymmetric-key cryptography: Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.

Introduction to Cryptography

Challenges of Cryptography:

While cryptography is a powerful tool for securing information, it also presents several challenges, including:

- Key management: Cryptography relies on the use of keys, which must be managed carefully to maintain the security of the communication.
- Quantum computing: The development of quantum computing poses a potential threat to current cryptographic algorithms, which may become vulnerable to attacks.
- Human error: Cryptography is only as strong as its weakest link, and human error can easily compromise the security of a communication.

Objectives of Cryptography

5. Access Control

- Regulates who can access and manipulate data.
- Enforced through permissions and cryptographic keys.

6. Key Management

- Involves the generation, distribution, storage, and destruction of cryptographic keys.
- Critical for maintaining security in cryptographic systems.

7. Secure Communication

- Enables safe transmission of information over insecure channels (e.g., the internet).
- Utilizes protocols like SSL/TLS for secure web communication.

Objectives of Cryptography

1. Confidentiality
- Protects information from unauthorized access.
- Achieved through encryption algorithms (e.g., AES, RSA).

2. Integrity
- Ensures data is not altered during transmission.
- Uses hash functions (e.g., SHA-256) to create a unique fingerprint of data.

3. Authentication
- Verifies the identities of parties involved in communication.
- Implemented through digital signatures and authentication protocols.

4. Non-repudiation :
- Prevents a party from denying the authenticity of their signature or a message.
- Ensured by using cryptographic methods like digital signatures.

Objectives of Cryptography

Applications of Cryptography:

- Secure Online Transactions: E-commerce, banking.
- Data Protection: Protecting sensitive information (e.g., health records).
- Digital Signatures: Verifying authenticity of digital documents.
- Secure Messaging: Apps like Signal and WhatsApp use end-to-end encryption.

Important Concepts:

- Encryption/Decryption: Process of converting plaintext to ciphertext and vice versa.
- Cipher: Algorithm for performing encryption and decryption.
- Key: A string of bits used by a cipher to encrypt and decrypt data.

Symmetric Key Encryption

In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. This means that both the sender and the receiver must have access to the secret key, which needs to be kept confidential to ensure security.

How It Works:

Encryption: The plaintext is combined with the secret key using a specific algorithm to produce ciphertext.
Decryption: The ciphertext is processed with the same key and algorithm to retrieve the original plaintext.

Example:
If P1 wants to send a secure message to P2, they would agree on a symmetric key (e.g., "mysecretkey"). P1 encrypts the message using this key, and sends the ciphertext to P2. P2 who has the same key, can then decrypt the message.

Symmetric Key Encryption

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other to decrypt.
The size of ciphertext is the same or smaller than the original plaintext.	The size of ciphertext is the same or larger than the original plaintext.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data needs to be transferred.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.

Symmetric Key Encryption

The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is lower as only one key is used for both encryption and decryption purposes.	Security is higher as two keys are used, one for encryption and the other for decryption.
Examples: 3DES, AES, DES and RC4	**Examples:** Diffie-Hellman, ECC, El Gamal, DSA and RSA

Steam Cipher

- A stream cipher is a method of encryption that encrypts plaintext one bit or byte at a time, producing ciphertext in a continuous stream.

- Stream Cipher follows the sequence of pseudorandom number stream.

- One of the benefits of following stream cipher is to make cryptanalysis more difficult, so the number of bits chosen in the Keystream must be long in order to make cryptanalysis more difficult.

- By making the key more longer it is also safe against brute force attacks.

- The longer the key the stronger security is achieved, preventing any attack.

- Keystream can be designed more efficiently by including more number of 1s and 0s, for making cryptanalysis more difficult.

Steam Cipher

Encryption :-

For Encryption,

- Plain Text and Keystream produces Cipher Text (Same keystream will be used for decryption.).
- The Plaintext will undergo XOR operation with keystream bit-by-bit and produces the Cipher Text.

Decryption :-

For Decryption,

- Cipher Text and Keystream gives the original Plain Text (Same keystream will be used for encryption.).
- The Ciphertext will undergo XOR operation with keystream bit-by-bit and produces the actual Plain Text.

Steam Cipher

Advantages of Stream Ciphers :-

- Speed
- Low complexity
- Sequential in nature
- Accessibility

Disadvantages of Stream Ciphers

- If an error occurs during transmission, it can affect subsequent bits, potentially corrupting the entire message because stream ciphers rely on previously stored cipher bits for decryption
- Maintaining and properly distributing keys to stream ciphers can be difficult, especially in large systems or networks.
- Some stream ciphers may be predictable or vulnerable to attack if their key stream is not properly designed, potentially compromising the security of the encrypted data.

Block Cipher

- Block cipher encrypts data in fixed-size blocks usually 64 or 128 bits at a time.
- The encryption algorithm processes each block of data separately using the cryptographic key to transform the plaintext into the ciphertext.
- Block ciphers function on complex mathematical computation and permutation to ensure that the data encrypted is safe.
- The choice of block size does not directly affect the strength of the encryption scheme.
- The strength of the cipher depends upon the key length. However, any size of the block is acceptable.

Steam Cipher vs Block Cipher

Block Cipher	Stream Cipher
Block Cipher Converts the plain text into cipher text by taking plain text's block at a time.	Stream Cipher Converts the plain text into cipher text by taking 1 bit plain text at a time.
Block cipher uses either 64 bits or more than 64 bits.	While stream cipher uses 8 bits.
The complexity of block cipher is simple.	While stream cipher is more complex.
Block cipher uses confusion as well as diffusion.	While stream cipher uses only confusion.
In block cipher, reverse encrypted text is hard.	While in-stream cipher, reverse encrypted text is easy.

Steam Cipher vs Block Cipher

Block cipher is slow as compared to a stream cipher.	While stream cipher is fast in comparison to block cipher.
Suitable for applications that require strong encryption, such as file storage and internet communications.	Suitable for applications that require strong encryption, such as file storage and internet communications.
More secure than stream ciphers when the same key is used multiple times.	Less secure than block ciphers when the same key is used multiple times.
key length is typically 128 or 256 bits.	key length is typically 128 or 256 bits.
Operates on fixed-length blocks of data.	Encrypts data one bit at a time.

AES

AES stands for Advanced Encryption Standard. It is a symmetric key encryption algorithm widely used to secure data. AES replaced the older DES (Data Encryption Standard) due to its strength and efficiency.

AES encryption uses various key lengths (128, 192, or 256 bits) to provide strong protection against unauthorized access.

This data security measure is efficient and widely implemented in securing internet communication, protecting sensitive data, and encrypting files.

The encryption process involves several rounds of transformations, where each round includes substitution, permutation, and mixing operations. The number of rounds depends on the key size:

- 10 rounds for AES-128
- 12 rounds for AES-192
- 14 rounds for AES-256

AES

Encryption :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

SubBytes: Each byte of the block is replaced using a predefined lookup table called the S-box (Substitution box). This step provides confusion, ensuring that small changes in input result in large, unpredictable changes in output.

ShiftRows: Rows of the state are shifted cyclically. The first row is unchanged, the second row is shifted by one byte, the third row by two bytes, and the fourth by three bytes.

MixColumns: The columns of the state are mixed to provide diffusion, meaning the output is spread across the entire block.

AddRoundKey: The state is XORed with a round key derived from the original key schedule.

AES

Decryption :

AES decryption is essentially the reverse of encryption. The rounds are performed in reverse order, and the transformations (like SubBytes) are applied using inverse operations.

The main steps are:

- **Inverse ShiftRows** (opposite of encryption’s ShiftRows)
- **Inverse SubBytes** (using the inverse S-box)
- **Inverse MixColumns** (applies the reverse mixing)
- **AddRoundKey** (as in encryption)

The decryption process is computationally similar but involves inverting each of the operations used during encryption.

DES

The Data Encryption Standard (DES) is a symmetric-key block cipher that was widely used for data encryption until it was deemed insecure due to advances in computing power.

Despite its weaknesses, DES played a crucial role in the development of modern cryptography and paved the way for stronger encryption algorithms, such as AES (Advanced Encryption Standard).

DES uses a 56-bit key for encryption. However, it is often represented as a 64-bit key, with 8 bits reserved for parity checks (error detection), leaving only 56 bits as the actual key used for encryption.

DES performs 16 rounds of encryption, where each round includes substitutions, permutations, and XOR operations.

DES

During each round, S-boxes (substitution boxes) are used to replace data values in a non-linear fashion. This substitution step helps to increase the complexity and security of the cipher.

After each round, a permutation step is applied to the data to further increase diffusion.

After completing all 16 rounds, the final output is a 64-bit block of ciphertext, which can be transmitted securely.

DES

Vulnerable to Brute-Force:

- With only 56-bit keys, DES is no longer secure against brute-force attacks.

Computational Power:

- With modern computing power, DES can be broken in a short amount of time.

Replaced by AES:

- AES (Advanced Encryption Standard) was introduced as a replacement for DES and provides much stronger security with larger key sizes (128, 192, and 256 bits).

DES

Triple DES (3DES):

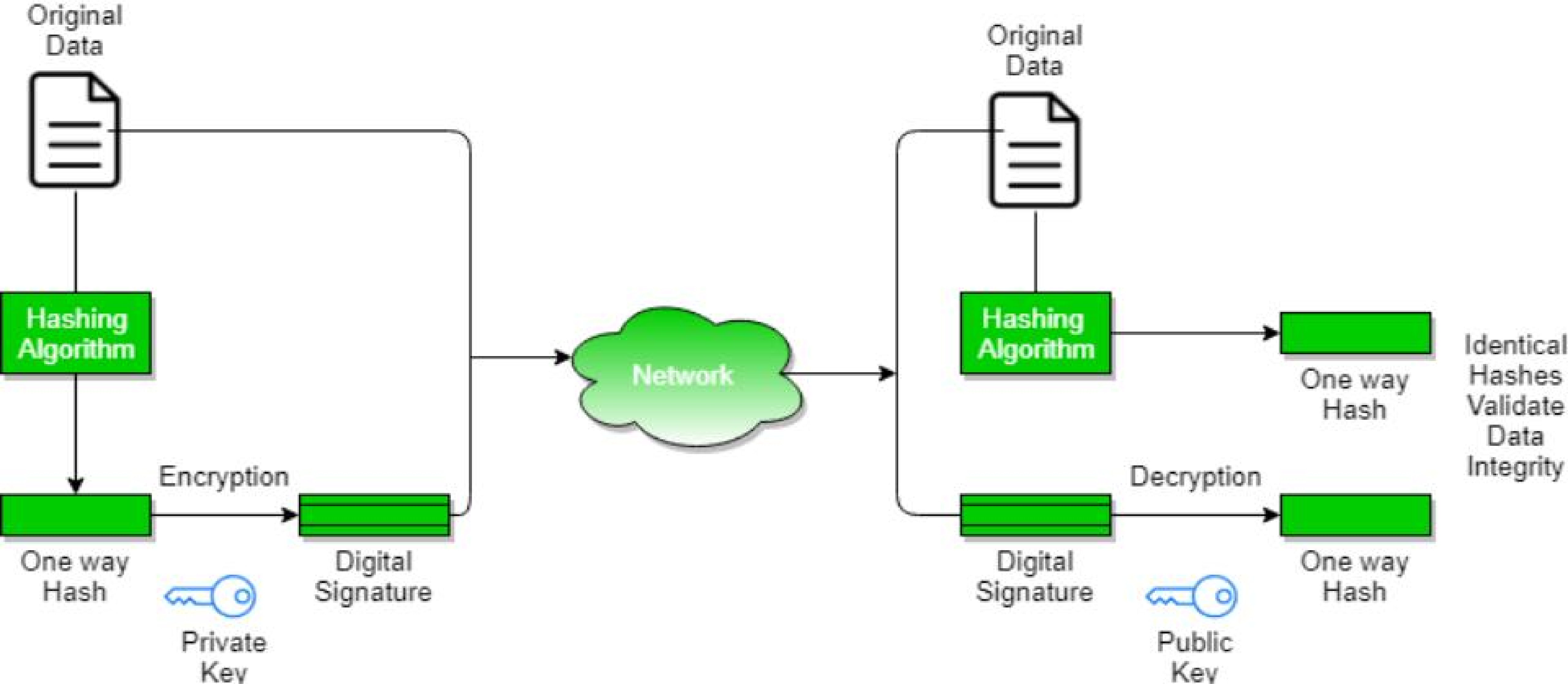
To enhance security, Triple DES (3DES) was introduced as a way to strengthen DES without needing to completely replace it. 3DES applies the DES algorithm three times with different keys:

- Encrypt the data with one key.
- Decrypt the result with a second key.
- Encrypt again with a third key.

This approach increases the effective key length to 168 bits (using three 56-bit DES keys). However, 3DES is still slower and not as secure as newer algorithms like AES.

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.



Digital Signature

To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed.

The signing algorithm then encrypts the hash value using the private key (signature key).

This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier.

The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed-length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.

Digital Signature

Verifier receives Digital Signature along with the data.

It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value.

It also applies the same hash function on the received data and generates a hash value. If they both are equal, then the digital signature is valid else it is invalid.

Completion of Unit-2

Your Questions

THANKS