Week 05:

**DATA ENCRYPTION STANDARD (DES)**

Developed by IBM and adopted by NIST in 1977

64-bit blocks and 56-bit keys

A symmetric encryption Algorithm

**3DES**

Nested application of DES with three different keys *KA*, *KB*, and *KC*

Key length is 168 bits,

*EKC*(*DKB*(*EKA*(*P*))); *P DKA*(*EKB*(*DKC*(*C*))) –

**Encrypt with Ka, decrypt with Kb and again encrypt with Kc.** Equivalent to DES when KA=KB=KC (backward compatible).

**ADVANCED ENCRYPTION STANDARD (AES)**

Selected by NIST

128-bit blocks

Possible key lengths: 128, 192 and 256 bits

AES-256 is the symmetric encryption algorithm of choice.

**BLOCK CIPHER MODES**

Describes the way a block cipher encrypts and decrypts a sequence of message blocks.

Strengths: Is very simple; Can tolerate the loss or damage of a block.

Weakness: Documents and images are not suitable for ECB encryption since patterns in the plaintext are repeated in the ciphertext

**CIPHER BLOCK CHAINING (CBC) MODE**

Each plaintext block is combined with the previous ciphertext block before encryption.

An initialization vector (IV), a random block, is separately transmitted and encrypted.

For decryption, each ciphertext block is decrypted and then combined with the previous ciphertext block to obtain the plaintext.

CBC mode is a symmetric encryption algorithm.

**RIVEST CIPHER 4 (RC4) - STREAM**

Designed by Ron Rivest for RSA Security, Trade secret.

Symmetric encryption algorithm.

2,048 bits keys

Simple algorithm and remarkable speed

**ASYMMETRIC CIPHERS: RSA**

Public key Cryptosystem that uses Block Cipher.

GK: RSA remains one of the most widely used and trusted cryptographic algorithms for secure communication and digital signatures in various applications, including SSL/TLS for secure web browsing, email encryption, and digital certificates.

**ONE TIME PAD (OTP)**

Extremely powerful type of substitution cipher.

Considered unbreakable.

Each pad in the scheme must be:

* Made up of truly random values
* Used only one time
* Securely distributed/generated for both sides
* Secured at sender’s and receiver’s sites
* At least as long as the message

One time Pad is a form of Stream Cipher.

A yellow and blue background with black text

Description automatically generated

To encrypt message stream XOR key stream

To decrypt key stream XOR cipher text

**KEY**: A key is a piece of information used to control the operation of a cryptographic algorithm, such as encryption or decryption.

**KEY SPACE:** Key space refers to the total number of possible keys that can be used with a specific cryptographic algorithm. It represents the range of possible values a key can take.

**KEY MANAGEMENT**: Key management involves the generation, distribution, storage, and revocation of cryptographic keys. It is essential for ensuring the security and integrity of encrypted data.

Most difficult and critical parts of a cryptosystem

**KEY DISTRIBUTION TECHNIQUES**

**PAPER DISTRIBUTION**

Requires no technology to use.

it relies on physical delivery and manual installation by a person.

**DIGITAL DISTRIBUTION**

Keys can be distributed electronically, for example, via CDs or email.

Requires protection during transmission to prevent interception or tampering.

Higher-level encryption may be used to protect keys during transit and storage.

The Internet Security relies on Keys distribution called public key infrastructure (PKI).

**HARDWARE DISTRIBUTION**

Keys Distributed via **hardware** such as a smart card, or a plug-in module.

The advantage is that no copies exist outside of these components.

Reduces the risk of unauthorized access since no copies exist outside of the designated hardware.

**PURPOSE OF PUBLIC KEY INFRASTRUCTURE (PKI)**

* PKI provides a mechanism for two parties to establish a trusted relationship, even if they have no prior knowledge of each other.
* PKI enhances trust, integrity, and security in electronic transactions by enabling secure communication, data encryption, and digital signatures.
* PKI framework is used to manage, create, store, and distribute cryptographic keys and digital certificates.

**DIFFIE-HELLMAN KEY EXCHANGE**

The Diffie-Hellman key exchange algorithm serves the purpose of enabling two users to securely exchange a secret key that can be used for subsequent encryption of messages.

Here's an explanation of the Diffie-Hellman key exchange process using the analogy of mixing paint colors:

1. Common Paint: Alice and Bob agree on using a large prime number and a base, which are public and known to everyone, just like common paint colors that are publicly available.

2. Secret Colours: Alice and Bob each choose a secret number (a private key) that they keep to themselves, like selecting secret paint colors that they don't share with anyone else.

3. Mixing Colours: Both Alice and Bob mix their chosen secret colors with the publicly agreed colors. This step represents each party combining their private key with the agreed-upon parameters.

4. Creating the Shared Secret: Alice and Bob exchange the colors they obtained after mixing, representing the exchange of their mixed keys over a public channel.

5. The Common Secret: Using their previously obtained mixed colors and their own secret colors, Alice and Bob each create a final mixed color (key). This represents the generation of the shared secret key.

6. Secure Communication: Now that Alice and Bob both have the same final mixed color (key), they can use it to exchange data securely, just like having a shared secret key.

The asymmetric algorithm based on modular logarithms used to establish and exchange asymmetric keys over an insecure medium is Diffie-Hellman.

**KEY DISTRIBUTION CENTRES /CERTIFICATE DISTRIBUTION SYS­TEM -** a crucial role in securely distributing cryptographic keys or certificates within a network.

Rather than each organization creating the infrastructure to manage its own keys, several hosts could agree to trust a **common key-distribution center (KDC)**

All parties within the network must trust the KDC.

With a KDC, each entity needs only one secret key pair, established between itself and the KDC.

Kerberos is a widely used authentication protocol that employs the concept of a KDC.

**HASH AND DIGITAL SIGNATURE -** Hash and digital signature mechanisms play critical roles in ensuring data integrity and authenticity.

Digital signatures combine elements of public key cryptography and hashing algorithms to provide secure authentication and verification of data.

Digital signatures, often represented as certificates, are typically stored and managed within a Public Key Infrastructure (PKI) domain, which ensures their accessibility and trustworthiness.

**CREATING A DIGITAL SIGNATURE INVOLVES TWO MAIN STEPS:**

* The original message or data is passed through a hashing algorithm, generating a unique hash value that represents the content of the message.
* The hash value is then encrypted using the sender's private key, forming the digital signature.

A message is said to be digitally signed if it's sent with a message digest encrypted with the sender's private key.

**UPON RECEIVING THE SIGNED MESSAGE, THE RECIPIENT CAN VERIFY ITS AUTHENTICITY AND INTEGRITY BY:**

* Decrypting the digital signature using the sender's public key to obtain the hash value.
* Calculating the hash value of the received message independently and comparing it with the decrypted hash value. If they match, it confirms the integrity and authenticity of the message.

**A blue screen with white text

Description automatically generated**

**DIGITAL CERTIFICATES**

X.509 certificates are designed to bind the identity of the owner of a public key to various pieces of information, including the public key itself, the hostname (or domain name), the issuer (the Certificate Authority or CA), and other relevant details.

**CRYPTANALYSIS**

a variety of methods used by hackers and cybersecurity experts to decipher encrypted data.

**Objective** is to break cryptographic security systems and gain access to the contents of encrypted messages, without necessarily having access to the secret key used to encrypt the messages.

**CRYPTANALYSIS METHODS**

**BRUTE FORCE ATTACK:** This method involves trying every possible key until the correct one is found.

Time-consuming and requires significant computational power, especially against systems with long and complex keys.

Using a strong encryption algorithm to protect the key is a way to prevent brute force attacks in symmetric encryption.

**DICTIONARY ATTACK:** This method involves the attacker using a list of common words, phrases, and previously leaked passwords to attempt to guess a password.

**FREQUENCY ANALYSIS:** Effective against simple substitution ciphers. It involves analysing the frequency of characters or groups of characters in the ciphertext and comparing them to the expected frequencies in the language of the plaintext.

**KNOWN PLAINTEXT ATTACK:** If the attacker has access to both the plaintext and its corresponding ciphertext, they might be able to deduce the key or identify a weakness in the encryption algorithm.

**DIFFERENTIAL CRYPTANALYSIS:** This method involves analysing the differences in the input that lead to differences in the output.

Used against block ciphers to find correlation that can help in deducing the key.

**RAINBOW TABLE ATTACK:** This method is used against hash functions and involves using precomputed tables of hash values to find plaintexts that produce certain hash values.

**QUANTUM COMPUTING:** Though still in its infancy, quantum computing poses a potential future threat to traditional cryptographic algorithms, as it could theoretically break many of the current encryption methods.