Cryptography : Conversion of data into a scambled code that is encrypted and sent across a private or public network

Objectives of Cryptography :
1. Authentication
2. Confidentiality
3. Integrity
4. Non Repudiation

Types of Cryptography :

1. **Symmetric Encryption** :
    1. Uses the same key for encryption and decryption
    2. Symmetric encryption is also known as **secret-key cryptography**,
    3. Can be implemented in application-specific integrated chip (ASIC).

2. **Asymmetric Encryption** :
    1. Uses the different key for encryption and decryption,
    2. Also known as **public key Cryptography**.

Government Access to Keys (GAK) :

1. Software companies will give copies of all keys to the government.
2. The government promises that it will hold on to the keys in a secure manner and only use them when a court issues a warrant to do so

Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow.

Encryption is the process of converting readable plaintext into an unreadable ciphertext using a set of complex algorithms that transform the data into blocks or streams of random alphanumeric characters.

Ciphers :

Ciphers are algorithms used to encrypt or decrypt the data
Encipherment is the process of converting plaintext into a cipher or code; the reverse process is called **Decipherment**

Types of Ciphers :

Classical Ciphers : Classical ciphers are the most basic type of ciphers, which operate on letters of the alphabet (A–Z).
Types of Classical Ciphers :
    1. Substitution Ciphers : replaces units of plaintext with ciphertext
    2. Transposition Ciphers : plaintext are rearranged

Modern Ciphers : They provide message secrecy, integrity, and authentication of the sender.
Types of Modern Ciphers :
    1. Based on the type of key used :
        1. Symmetric key algorithm
        2. Asymmetric key algorithm
    2. Based on the type of input data
        1. Block cipher : operating on a block (a group of bits) of fixed size
        2. Stream Cipher : Symmetric-key ciphers are plaintext digits combined with a key stream

Data Encryption Standard (DES) :

- DES is a standard for data encryption that uses a **secret key** for both encryption and decryption
- DES uses a **64-bit secret key**, of which **56 bits are generated randomly** and the other **8 bits** are used for **error detection.**
- It uses a **data encryption algorithm (DEA)**, a **secret key block cipher** employing a **56-bit key** operating on 64-bit blocks.
- DES is the **archetypal block cipher**—an algorithm that takes a **fixed-length** string of plaintext bits and transforms it into a ciphertext bit string of the **same length.**

Triple Data Encryption Standard (DES) :

- Applying the same DES algorithm three times
- first option, all three keys are independent and different.
- In the second option, K1 and K3 are identical.
- In the third option, all three keys are the same;

Advanced Encryption Standard (AES) :

- **Symmetric-key algorithm**: both encryption and decryption are performed using the **same key**
- It is an iterated block cipher that works by repeating the defined steps multiple times
- It has a 128-bit block size, with key sizes of 128, 192, and 256 bits for AES-128, AES-192, and AES-256

RC4, RC5, and RC6 Algorithms :

RC4 :
- RC4 is a variable key-size **symmetric-key stream cipher**
- RC4 enables safe communications such as for **traffic encryption** (which secures websites) and for websites that use the SSL protocol.

RC5 :
- It is a **parameterized algorithm** with a variable block size, variable key size, and variable number of rounds.
- The encryption routine has three fundamental operations: **integer addition, bitwise XOR, and variable rotation.**
- The key size is **128 bits**

RC6 :
RC6 is a symmetric key block cipher derived from RC5 with
Two additional features:
    - integer multiplication (which is used to increase the **diffusion**, achieved in fewer rounds with increased **speed** of the cipher)
    - four 4-bit working registers (RC5 uses two 2-bit registers)

Digital Signature Algorithm (DSA) :
The DSA helps in the **generation** and **verification** of digital signatures for sensitive and unclassified applications.
Processes involved in DSA:
Signature Generation Process: The private key is used to know who has signed it.
Signature Verification Process: The public key is used to verify whether the given digital signature is genuine.

Digital Signature:
A digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the **signatory** and **integrity** of the data can be verified

DSA is a **public-key cryptosystem**

Rivest Shamir Adleman (RSA) :
A public-key cryptosystem for Internet encryption and authentication.
It uses modular arithmetic and elementary number theories to perform computations using two large prime numbers

Diffie–Hellman :
Cryptographic protocol that allows two parties to establish a shared key over an insecure channel
The Diffie–Hellman algorithm does not provide any authentication for the key exchange and is vulnerable to many cryptographic attacks.

Message Digest (One-way Hash) Functions :

- Hash functions calculate a unique fixed-size bit string representation called a message digest of any arbitrary block of information
- Message digest functions are also called **one-way hash** functions because they produce values that are nearly impossible to invert, resistant to attack, mostly unique, and widely distributed.
- The main role of a cryptographic hash function is to provide integrity in document management.

Message Digest Function: MD5 and MD6 :

- The MD5 algorithm takes a message of arbitrary length as the input and then outputs a **128-bit** fingerprint or message digest of the input
- MD5 is not **collision resistant**
- MD6 uses a **Merkle tree-like** structure to allow for immense parallel computation of hashes for very long inputs. It is resistant to differential cryptanalysis attack
- MD5 and MD6 are deployed for digital signature applications, file integrity checking, and storing passwords

Secure Hashing Algorithm (SHA) :

This algorithm generates a cryptographically secure one-way hash;

SHA-1 :
It produces a **160-bit** digest from a message with a maximum length of (264 – 1) bits, and it resembles the MD5 algorithm

SHA-2 :
It is a family of two similar hash functions with different block sizes, namely, **SHA-256**, which uses **32-bit words,** and **SHA-512,** which uses **64-bit words**

SHA-3 :
SHA-3 uses the **sponge construction,** in which message blocks are **XORed** into the initial bits of the state, which is then invertibly permuted

RIPEMD-160 and HMAC :

RIPEMD-160 :

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) is a 160-bit hash algorithm
There exist 128-, 256-, and 320-bit versions of this algorithm, which are called RIPEMD-128, RIPEMD-256, and RIPEMD-320,
The compression function consists of 80 stages made up of 5 blocks that execute 16 times each
This process repeats twice by combining the results at the bottom using modulo 32 addition

HMAC :

- HMAC is a type of **message authentication code (MAC)** that combines a cryptographic key with a cryptographic hash function
- It is widely used to verify the **integrity** of the **data** and **authentication** of a message
- This algorithm includes an embedded hash function, such as SHA-1 or MD5
- The **strength** of HMAC depends on the **embedded hash function**, **key size**, and the **size of the hash output**
- As HMAC executes the underlying hash function **twice**, it protects from various length extension attacks

Public Key Infrastructure (PKI) :

- PKI is a security architecture developed to increase the confidentiality of information exchanged over the insecure Internet.
- It includes hardware, software, people, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.
- The PKI helps to bind public keys with corresponding user identities by means of a **certification authority (CA).**

Components of PKI :

- **Certificate Management System**: Generates, distributes, stores, and verifies certificates
- **Digital Certificates**: Establishes credentials of a person when performing online transactions
- **Validation Authority (VA)**: Stores certificates (with their public keys)
- **Certification Authority (CA):** Issues and verifies digital certificates
- **End User:** Requests, manages, and uses certificates
- **Registration Authority (RA)**: Acts as the verifier for the CA

Signed Certificate (CA) vs. Self-Signed Certificate:

Signed Certificate :

- User approaches a trustworthy **certification authority (CA)** and purchases a digital certificate
- User gets the public key from the CA and signs the document using it
- The receiver can verify the certificate by enquiring with **validation authority (VA)**
- VA verifies the certificate to the receiver, but it does not share the **private key**

Self-Signed Certificate :

- User creates public and private keys using a tool, such as Adobe Acrobat Reader, Java's keytool, or Apple's Keychain
- User uses public key to sign the document
- The self-signed document is delivered to the receiver
- The receiver request the private key from the user
- User shares the private key with the receiver

Digital Signature :

- Digital signature uses asymmetric cryptography to simulate the security properties of a signature in digital rather than written form
- A digital signature may be further protected by encrypting the signed email for confidentiality

Secure Sockets Layer (SSL) :

- The **Secure Sockets Layer (SSL)** protocol is an **application layer protocol** for managing the security of **message transmission** on the Internet.
- It provide a secure authentication mechanism between **two** communicating applications
- SSL requires a **reliable transport protocol,** such as **TCP**, for data transmission and reception.
- It uses **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections

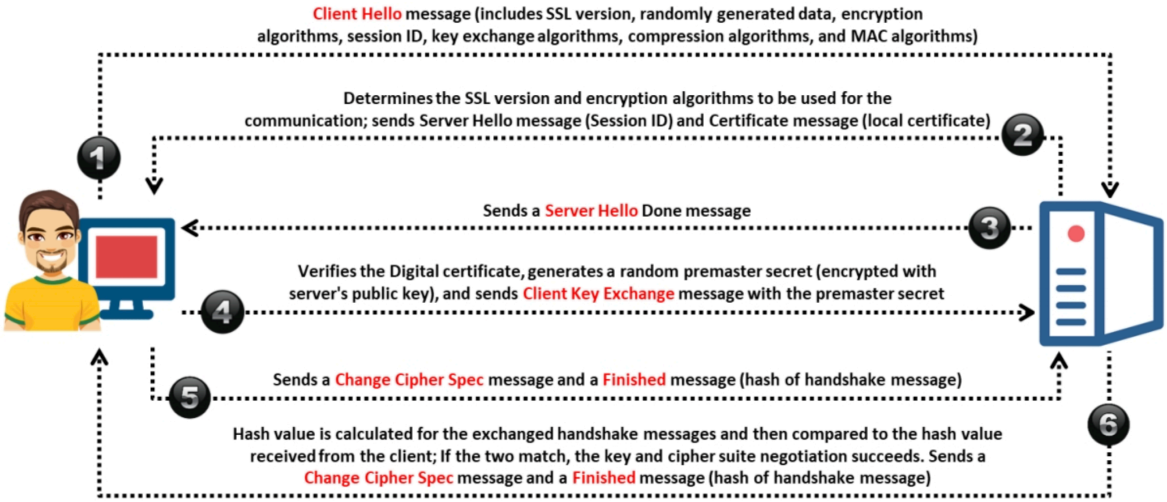

Figure 20.25: SSL handshake protocol flow

Transport Layer Security (TLS) :

The **Transport Layer Security (TLS)** protocol is used to establish a secure connection between a client and a server and ensure the **privacy** and **integrity** of information during **transmission**.

It uses a **symmetric** key for bulk encryption, **asymmetric** key for **authentication** and key exchange, and **message authentication codes** for message integrity

It uses the RSA algorithm with 1024-and 2048-bit strengths

Pretty Good Privacy (PGP) :

- **Pretty Good Privacy (PGP)** is a protocol used to **encrypt** and **decrypt data** with **authentication** and **cryptographic privacy**.
- It is often used for **data compression, digital signing, encryption** and **decryption of messages, emails, files, and directories,** and to enhance the privacy of **email communications**.
- The algorithm used for message encryption is **RSA** for key transport and **IDEA** for bulk-message encryption.

PGP is used for:

? Encrypting a message or file prior to transmission so that only the recipient can decrypt and read it
? Clear signing of the plaintext message to ensure the authenticity of the sender
? Encrypting stored computer files so that no one besides the person who encrypted them can decrypt them
? Deleting files rather than just removing them from the directory or folder
? Data compression for storage or transmission

GNU Privacy Guard (GPG) :

- GNU Privacy Guard (GPG) is a **software replacement of PGP** and free implementation of the **OpenPGP** standard that is used to encrypt and decrypt data.
- **GPG** is also called a **hybrid encryption software program**, as it uses **both** symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange, which is achieved using the receiver's public key for encrypting the session key.
- It also supports **S/MIME** and **Secure Shell (SSH)**

Web of Trust (WOT) :

- Web of trust (WoT) is a trust model of **PGP, OpenPGP,** and **GnuPG** systems
- Everyone in the network is a **Certificate Authority (CA)** and signs for other trusted entities
- WoT is a chain of a network in which individuals intermediately validate each other's certificates using their signatures
- Every user in the network has a **ring of public keys** to encrypt the data, and they introduce many other users whom they trust

Disk Encryption :

Disk encryption is a technology that protects the **confidentiality** of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware

Cryptanalysis :

Cryptanalysis is the study of ciphers, ciphertext, or cryptosystems with the ability to identify vulnerabilities in them and thus extract plaintext from ciphertext even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

Cryptanalysis Methods :

1. Linear Cryptanalysis :

- Commonly used on block ciphers
- It is a known plaintext attack and uses a linear approximation to describe the behavior of the block cipher

2. Differential Cryptanalysis

Differential cryptanalysis is a form of cryptanalysis applicable to symmetric key algorithms

3. Integral Cryptanalysis

This attack is particularly useful against block ciphers based on substitution-permutation networks as an extension of differential cryptanalysis

Code Breaking Methodologies :

1. **Brute Force** : Cryptography keys are discovered by trying every possible combination

2. **Frequency Analysis** :

The study of the **frequencies** of letters or groups of letters in a ciphertext
It works based on the fact that in any given stretch of written language, certain letters and combinations of letters occur with varying frequencie

3. **Trickery and Deceit** : Involves the use of social engineering techniques to extract cryptography keys

4. **One-Time Pad** : A one-time pad contains many non-repeating groups of letters or number keys, which are chosen randomly.

Rubber Hose Attack : Extraction of cryptographic secrets (e.g., the password to an encrypted file) from a person by coercion or torture.

Birthday Attack : A birthday attack is the name used to refer to a class of brute-force attacks against cryptographic hashes that makes the brute forcing easier

Birthday paradox: The probability that two or more people in a group of 23 share the same birthday is greater than 0.5

Meet-in-the-Middle Attack on Digital Signature Schemes. :
The attack works by encrypting from one end and decrypting from the other end, thus meeting in the middle
It can be used for forging messages that use multiple encryption schemes

Side-channel attack :
A side-channel attack is a physical attack performed on a cryptographic device/cryptosystem to gain sensitive information.
At the time of decryption in a cryptosystem, physical environmental factors, such as **timing** and **power dissipation**, **acting** on the components of a computer are recorded by an attacker

Rainbow Table Attack
A rainbow table attack is a type of cryptography attack whereby an attacker uses a rainbow table for reversing cryptographic hash functions.

Related Key Attack :
An attacker launch a related key attack by exploiting the **mathematical relationship** between keys in a cipher to gain access over encryption and decryption functions

Key Stretching :
Key stretching refers to the process of strengthening a key that might be slightly too weak, usually by making it longer

PBKDF2 (Password-Based Key Derivation Function 2) is a part of PKCS #5 v. 2.01. It applies some function (such as hash or HMAC) to the password or passphrase along with Salt to produce a derived key

bcrypt is used with passwords; it essentially uses a derivation of the Blowfish algorithm, converted to a hashing algorithm to hash a password and add Salt to it