Cryptography

- Cryptography is the conversion of data into a scrambled code that is encrypted and sent across a private or public network
- Cryptography is used to protect confidential data, such as email messages, chat sessions, web transactions, personal data, corporate data, and e-commerce applications

Objectives of Cryptography

- Confidentiality
- Integrity
- Authentication
- Non-redpudiation

Cryptographic Process

- **Plaintext** (readable format) is encrypted by means of encryption algorithms such as RSA, DES, and AES, resulting in a **ciphertext** (unreadable format) that, on reaching the destination, is decrypted into readable plaintext.

Symmetric Encryption

- **Symmetric Encryption** (secret-key, shared-key) uses the same key for encryption as it does for decryption.

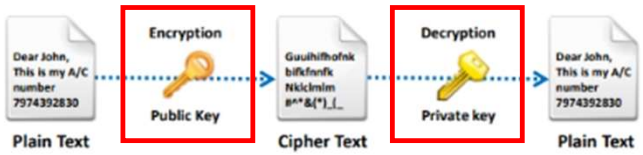
- Symmetric encryption requires that both the sender and the receiver of the message possess the same encryption key.
- The sender uses a key to encrypt the plaintext and sends the resultant ciphertext to the recipient, who uses the same key (used for encryption) to decrypt the ciphertext into plaintext.

Symmetric Encryption

- How do you get the second party the key if you've never met them?
  - Trusted Third Party, Key Escrow
- Need a new key for every person you wish to communicate with
  - Alice and Bob (Key 1)
  - Alice and Carol (Key 2)
  - Alice and Dave (Key 3)
  - Etc
- No non-repudiation, integrity, or authentication
- Relying on the security of others to guard your communication.
- Two people can keep a secret only if one of them is dead.

Asymmetric Encryption

- **Asymmetric Encryption** (public-key) uses different encryption keys, which are called public and private keys for encryption and decryption.



- The public key is publicly available to anyone.
- The private key is secret and held only by the key owner
- Provides confidentiality, integrity, authentication, and nonrepudiation in data management

Asymmetric Encryption

- Asymmetric encryption uses the following sequence to send a message:
  1. An individual finds the public key of the person he or she wants to contact in a directory.
  2. This public key is used to encrypt a message that is then sent to the intended recipient.
  3. The receiver uses the private key to decrypt the message and reads it
- Provides confidentiality
- Can be combined with other techniques to provide non-repudiation, integrity, and authentication

Asymmetric Encryption

- A ciphertext generated by using a public key can only be decrypted by the corresponding private key.
- A ciphertext generate using the private key can be decrypted by **anyone** using the public key.

Strengths and Weaknesses of Crypto Methods

	Symmetric Encryption	Asymmetric Encryption
Strengths	Faster and easier to implement, as the same key is used to encrypt and decrypt data Requires less processing power Can be implemented in application-specific integrated chip (ASIC).	Convenient to use, as the distribution of keys to encrypt messages is not required
	Prevents widespread message security compromise as different secret keys are used to communicate with different parties	Enhanced security, as one need not share or transmit private keys to anyone
	The key is not bound to the data being transferred on the link; therefore, even if the data are intercepted, it is not possible to decrypt it	Provides digital signatures that cannot be repudiated
Weaknesses	**Symmetric Encryption**	**Asymmetric Encryption**
	Lack of secure channel to exchange the secret key	Slow in processing and requires high processing power
	Difficult to manage and secure too many shared keys that are generated to communicate with different parties	Widespread message security compromise is possible (i.e., an attacker can read complete messages if the private key is compromised)
	Provides no assurance about the origin and authenticity of a message, as the same key is used by both the sender and the receiver	Messages received cannot be decrypted if the private key is lost
	Vulnerable to dictionary attacks and brute-force attacks	Vulnerable to man-in-the-middle and brute-force attacks

Government Access to Keys (GAK)

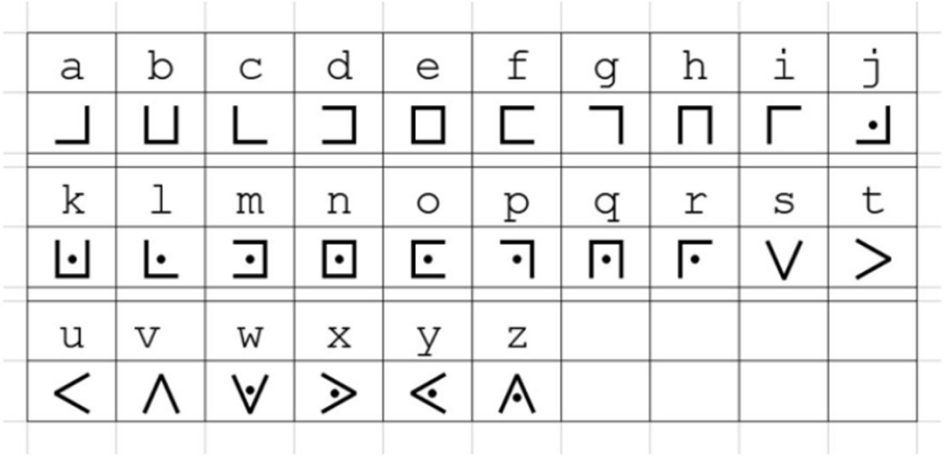
- GAK means that software companies will give copies of all keys (or at least a sufficient proportion of each key that the remainder could be cracked) to the government
- The government promises that it will hold on to the keys in a secure manner and only use them when a court issues a warrant to do so.
  - To the government, this issue is similar to the ability to wiretap phones.
- Government agencies are responsible for protecting these keys. Such agencies generally use a single key to protect other keys, which is not a good idea, as revealing a single key could expose the other keys.

Cyphers

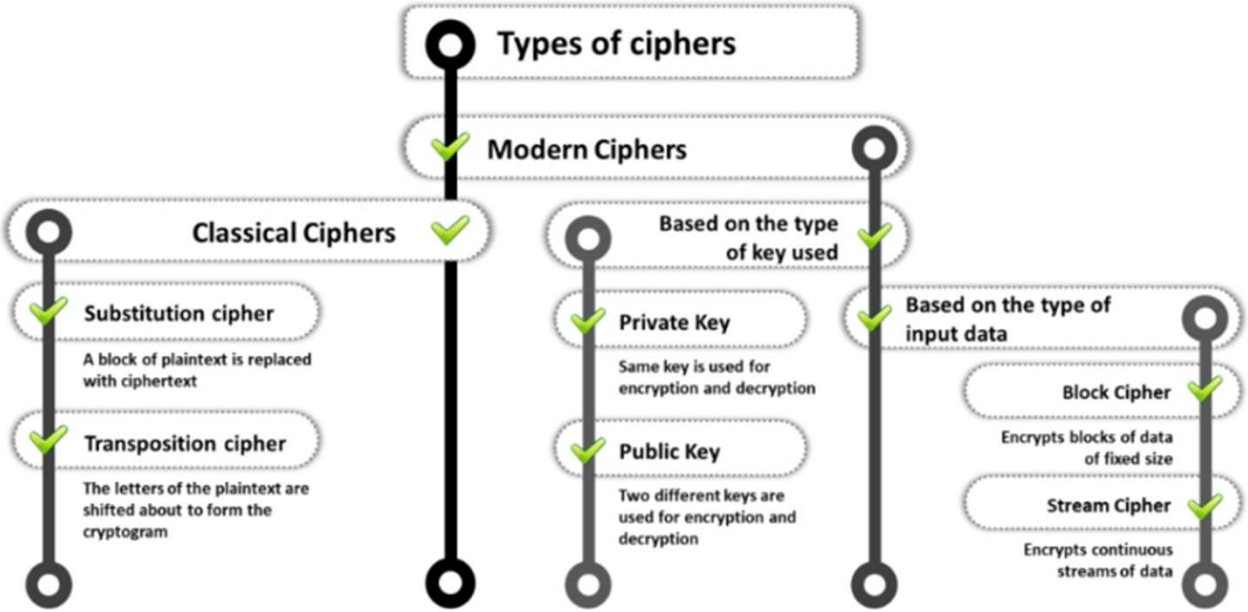
- A **cipher** is an algorithm (a series of well-defined steps) for performing encryption and decryption.
- Encipherment is the process of converting plaintext into a cipher or code; the reverse process is called decipherment.
- A message encrypted using a cipher is rendered unreadable unless its recipient knows the secret key required to decrypt it..

A Cipher is NOT a Code

- A **code** is a system of rules to convert information—such as a letter, word, sound, image, or gesture—into another form, sometimes shortened or secret.
- A code **requires** a codebook.



Types of Ciphers



Classical Ciphers

- Classical ciphers are the most basic type of ciphers, which operate on letters of the alphabet (A–Z).
- These ciphers are generally implemented either by hand or with simple mechanical devices.
- Provide only confidentiality.
- Because these ciphers are easily deciphered, they are generally unreliable.

Type of Classical Ciphers

- Substitution Cipher: The user replaces units of plaintext with ciphertext according to a regular system. For example, “HELLO WORLD” can be encrypted as “PSTER HGFST” (i.e. H=P, E-S, etc)

- Transposition Cipher: Letters in the plaintest are rearranged according to a regular system to product the cupher text. For example, ROT13 or Caesar Cipher

Modern Ciphers

- Designed to withstand a wide range of attacks.
- They provide message secrecy, integrity, and authentication of the sender.
- Symmetric-key algorithms (Private-key cryptography): Use the same key for encryption and decryption.
- Asymmetric-key algorithms (Public-key cryptography): Use two different keys for encryption and decryption.

Modern Ciphers

- **Block Cipher**: Deterministic algorithms operating on a block (a group of bits) of fixed size with an unvarying transformation specified by a symmetric key.
- Most modern ciphers are block ciphers. They are widely used to encrypt bulk data.
- Examples include DES, AES, IDEA, etc.
- When the block size is less than that used by the cipher, padding is employed to achieve a fixed block size.

Modern Ciphers

- **Stream Cipher:** Symmetric-key ciphers are plaintext digits combined with a key stream (pseudorandom cipher digit stream). The user applies the key to each bit, one at a time.
- Examples include RC4, SEAL, etc.

Data Encryption Standard (DES)

- DES is BROKEN and should not be used.
- Symmetric cryptosystem
- DES uses a 64-bit secret key, of which 56 bits are generated randomly and the other 8 bits are used for error detection.
- DES provides 72 quadrillion or more possible encryption keys
- 3DES (Triple DES) was developed while a search for a new standard was conducted

Advanced Encryption Standard (AES)

- The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data.
- AES consists of a symmetric-key algorithm: both encryption and decryption are performed using the same key.
- The design of AES makes its use efficient in both software and hardware.

Rivest–Shamir–Adleman (RSA)

- RSA is a public-key cryptosystem (asymmetric) for Internet encryption and authentication.
- RSA uses modular arithmetic and elementary number theories to perform computations using two large prime numbers.
- Cryptography uses RSA for public key encryption and for a digital signature (to sign a message and verify it).
- The RSA signature scheme is the first technique used to generate digital signatures.
- Can get confidentiality, authentication, integrity and non-repudiation

Problems with asymmetric key schemes

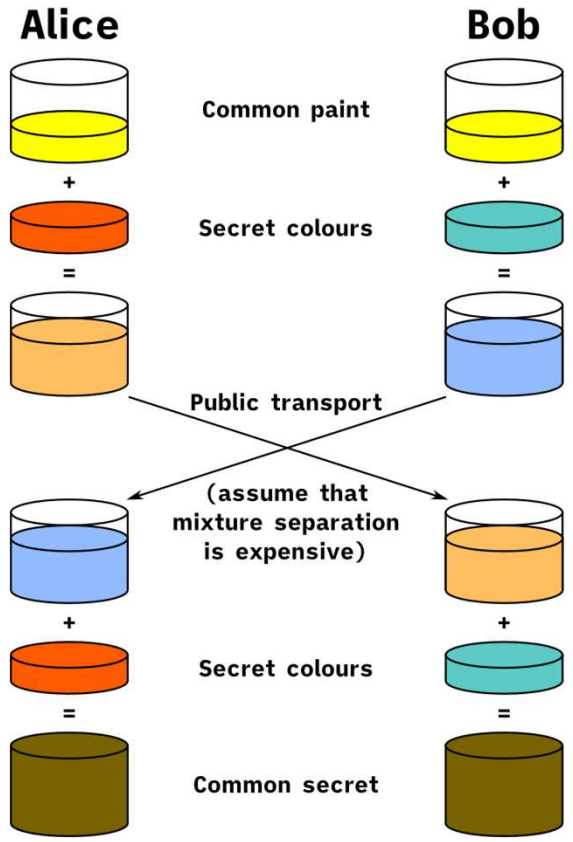
- They are too slow for encrypting internet traffic.
- BUT, symmetric keys have to be pre-shared and a key management nightmare
- But:
  1. How can I symmetrically encrypt my internet traffic with my bank without exchanging keys ahead of time?
  2. How do I know the bank website is actually my bank?

Diffie-Hellman key exchange

- A cryptographic protocol that allows two parties to establish a shared key over an insecure channel.
- It was developed and published by Whitfield Diffie and Martin Hellman in 1976.
- Actually, it was independently developed a few years earlier by Malcolm J. Williamson of the British Intelligence Service, but it was classified at that time.

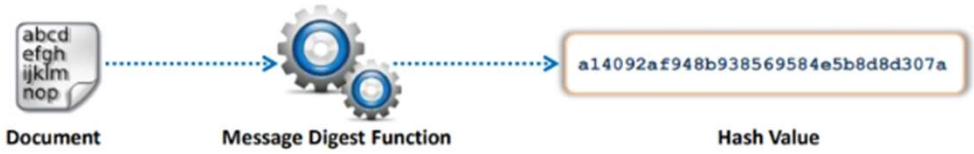
Diffie-Hellman key exchange

- Both parties can develop the same shared key.
- Even is a third party intercepts the common paint and public exchange they still can not construct the same key.



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 distill the information contained in a file (small or large) into a single fixed-length number.
- 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



Message Digest (One-Way Hash) Functions

- The main role of a cryptographic hash function is to provide integrity in document management. Cryptographic hash functions are an integral part of digital signatures.
- Their main purpose is to calculate the signature of the document's hash value, which is smaller than the document
- Widely used message digest functions include the following algorithms:
  - MD5 – MD5 is BROKEN do not use for anything serious
  - SHA
- Provides integrity

Digital Signatures

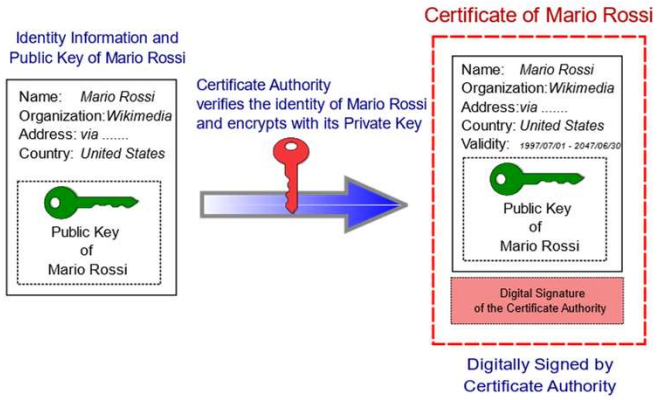
- A digital signature uses asymmetric cryptography and a one-way hash to provide non-repudiation and integrity.
- The document is hashed and the hash is encrypted with the signers private key.
- The recipient hashes the received document. They then decrypt the encrypted hash with the senders public key.
  - If the two hashes don't match then the document was modified since the sender signed it.

Digital Signatures

- A digital signature uses asymmetric cryptography and a one-way hash to provide non-repudiation and integrity.
- The document is hashed and the hash is encrypted with the signers private key.
- The recipient hashes the received document. They then decrypt the encrypted hash with the senders public key.
  - If the two hashes don't match then the document was modified since the sender signed it.

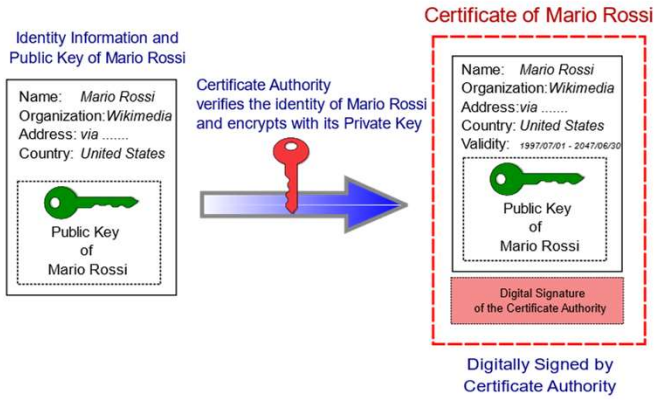
Verifying Website

- Digital Signatures form the basis for verifying the identity of a remote website.
- A Certificate Authority verifies the owner of a domain and encrypts the domain owners public key with the CA's private key.



Verifying Website

- Digital Signatures form the basis for verifying the identity of a remote website.
- A Certificate Authority verifies the owner of a domain and encrypts the domain owners public key with the CA's private key.



Verifying Website

- By issuing the certificate, the CA confirms or validates that the public key contained in the certificate belongs to the person, company, server, or other entity mentioned in the certificate.
- The CA accepts responsibility for saying, “Yes, this person is who they state they are, and we, the CA, certify that.”
- Your browser receives the certificate from the website and decrypts it using the CA’s public key. You will now have the public key of the website and confirmation the website is who they say they are.
- Using the public key of the website you can now send do a Diffie-Hellman key exchange to generate a symmetric key for the session.