Encryption

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-repudiation

Cryptographic Process

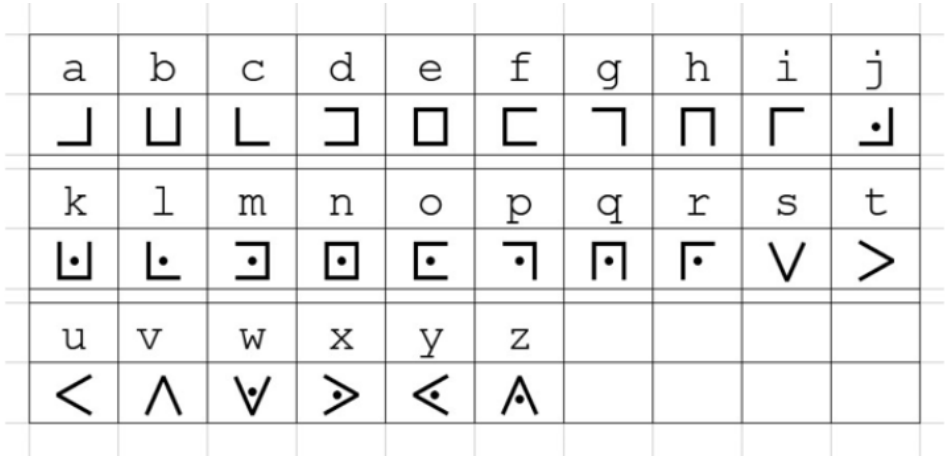
- **Plaintext** (readable format) is encrypted by means of encryption algorithms such as RSA, DES, and AES, resulting in a **ciphertext** (unreadable format) that, on reaching the destination, is decrypted into readable plaintext.

Ciphers

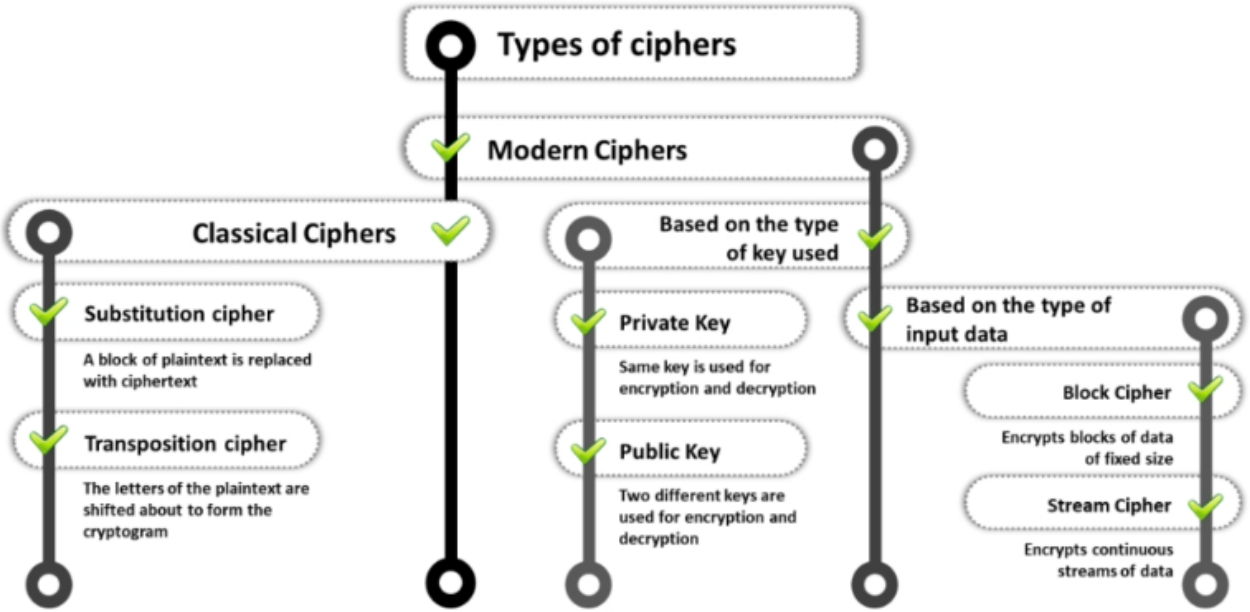
- A **cipher** is an algorithm (a series of well-defined steps) for performing encryption and decryption.
- Encipherment is the process of converting plaintext into a cipher or code; the reverse process is called decipherment.
- A message encrypted using a cipher is rendered unreadable unless its recipient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

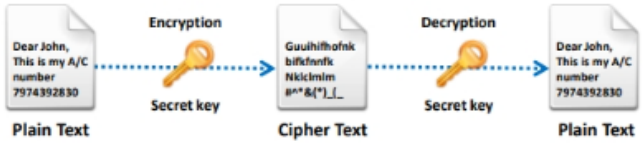
- **Stream Cipher:** Symmetric-key ciphers are plaintext digits combined with a key stream (pseudorandom cipher digit stream). The user applies the key to each bit, one at a time.
- Examples include RC4, SEAL, etc.

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.

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

- Need a strong algorithm
  - Even an opponent who knows the algorithm and has a cypiertext can not decrypt it
- Sender and Receiver must have pre-shared a secret key

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.

Attacking Symmetric Encryption

- Cryptanalysis - exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.

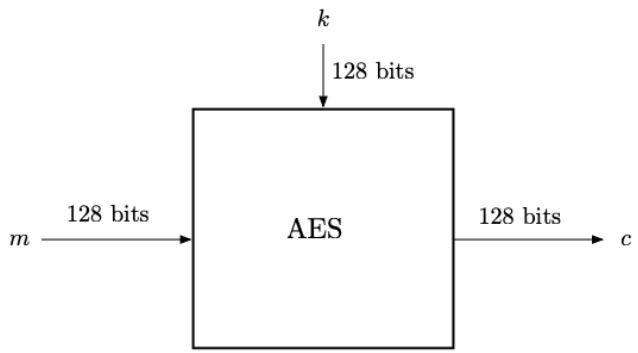
- Brute-Force Attack - try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
  - On average, half of all possible keys must be tried to achieve success.

Brute-Force Attacks

- Unless known plaintext is provided, the analyst must be able to recognize plaintext as plaintext.
- If the message is just plain text in English, then the result pops out easily, although the task of recognizing English would have to be automated.
- If the text message has been compressed before encryption, then recognition is more difficult.
- If the message is some more general type of data, such as a numerical file, and this has been compressed, the problem becomes even more difficult to automate.

Symmetric Block Encryption Algorithms

- A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for ϵ



A secure block cipher should be computationally indistinguishable from a random permutation.

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

Data Encryption Standard (DES)

- Two concerns over DES strength
  - Strength of the algorithm - Over the years, there have been numerous attempts to find and exploit weaknesses in the algorithm, making DES the most-studied encryption
    - Despite numerous approaches, no one has so far reported a fatal weakness in DES.

Data Encryption Standard (DES)

- Two concerns over DES strength
  - Small size of the key - a key length of 56 bits, there are 256 possible keys, which is approximately 7.2 * 1016 keys.

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/μs	Time Required at 10^{13} decryptions/μs
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55}\,\mu s = 1.125$ years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127}\,\mu s = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167}\,\mu s = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191}\,\mu s = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255}\,\mu s = 1.8 \times 10^{60}$ years	1.8×10^{56} years

Triple Data Encryption Standard (3DES)

- 3DES (Triple DES) was developed while a search for a new standard was conducted.
- Involves repeating the basic DES algorithm three times, using either two or three unique keys, for a key size of 112 or 168 bits
- Benefits:
  - With its 168-bit key length, it overcomes the vulnerability to brute-force attack of DES.
  - The underlying encryption algorithm in 3DES is the same as in DES.

BUT, it's SLOW

Advanced Encryption Standard (AES)

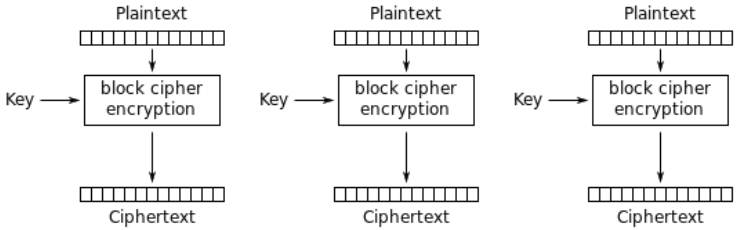
- The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data.
- AES consists of a symmetric-key algorithm: both encryption and decryption are performed using the same key.
- The design of AES makes its use efficient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

Advanced Encryption Standard (AES)

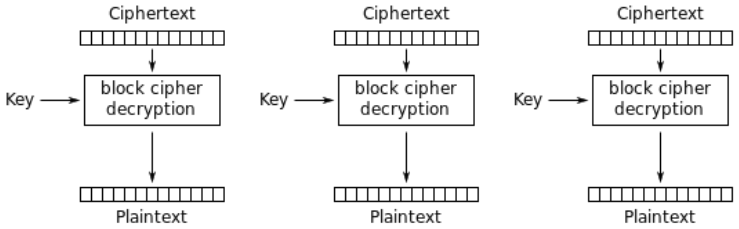
- Has a block length of 128 bits and support for key lengths of 128, 192, and 256 bits
- If we want to encrypt longer messages we break up a long message into a sequence of data blocks, and encrypt each data block separately. This is called electronic codebook mode, or ECB mode for short.

Electronic Codebook (ECB)

- The message is divided into blocks, and each block is encrypted separately.



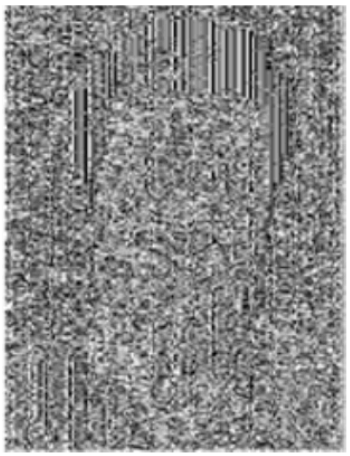
Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

Problems with ECB

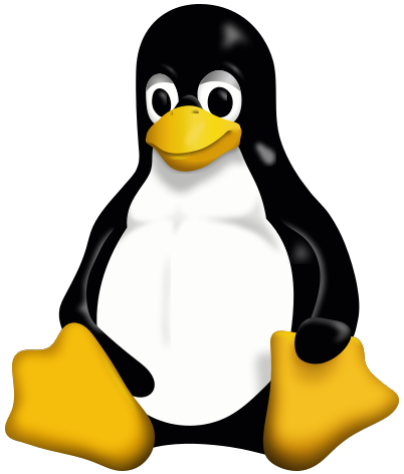
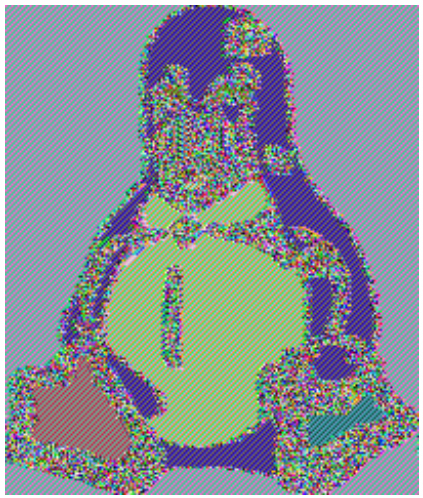
(a) plaintext



(b) plaintext encrypted in ECB mode using AES

- Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well.
- ECB is not recommended for use in cryptographic protocols

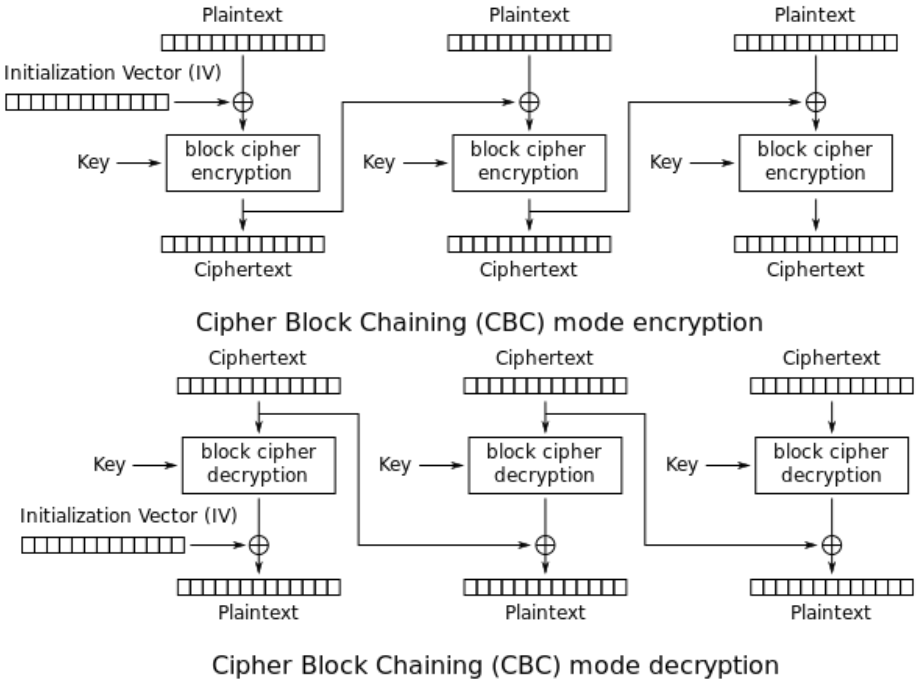
Problems with ECB


- Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well.
- ECB is not recommended for use in cryptographic protocols

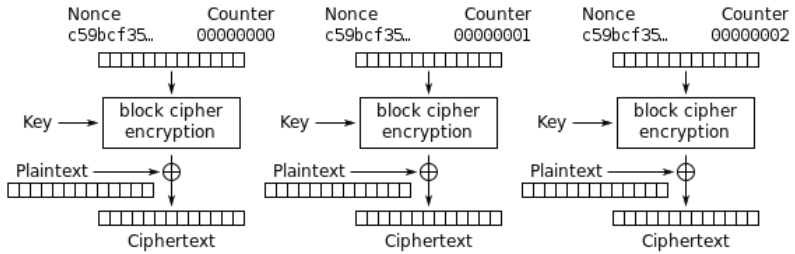
Cipher Block Chaining (CBC)

- A historically important encryption method is to use a block cipher in cipher block chaining (CBC) mode.
- In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.
- Each ciphertext block depends on all plaintext blocks processed up to that point.

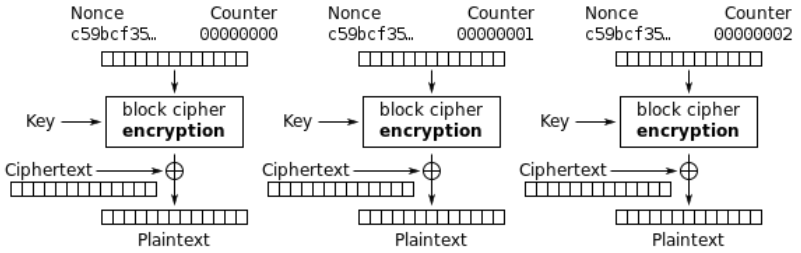


Counter Mode (CTR)

- Counter mode turns a block cipher into a stream cipher.
- It generates the next keystream block by encrypting successive values of a "counter".
- The counter can be any function which produces a sequence which is guaranteed not to repeat for a long time, although an actual increment-by-one counter is the simplest and most popular.



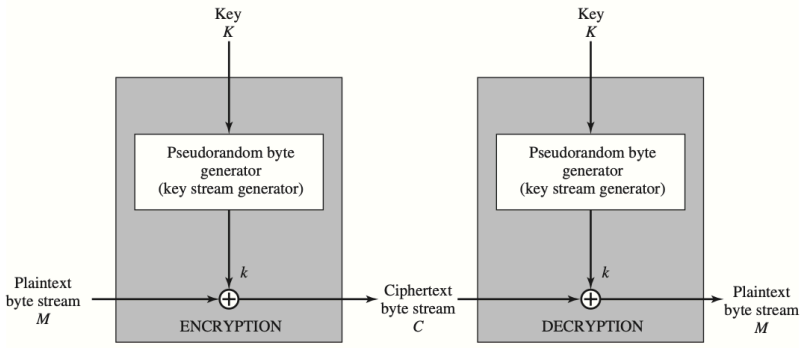
Counter (CTR) mode encryption



Counter (CTR) mode decryption

Stream Cyphers

- A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.
- A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time.



(b) Stream encryption

Block vs. Stream Cyphers

- The advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers.
- The advantage of a block cipher is that you can reuse keys.
- For applications that require encryption/decryption of a stream of data, such as over a data communications channel or a browser/ Web link, a stream cipher might be the better alternative.
- For applications that deal with blocks of data, such as file transfer, e-mail, and database, block ciphers may be more appropriate.

One-Time Pad

- The one-time pad (OTP) is an encryption technique that cannot be cracked, but requires the use of a single-use pre-shared key that is larger than or equal to the size of the message being sent.
- A plaintext is paired with a random secret key. Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition.

One-Time Pad

- The resulting ciphertext will be impossible to decrypt or break if the following four conditions are met:
  1. The key must be at least as long as the plaintext.
  2. The key must be random (uniformly distributed in the set of all possible keys and independent of the plaintext), entirely sampled from a non-algorithmic, chaotic source such as a hardware random number generator; patternless, according to Gregory Chaitin definition. It is not sufficient for OTP keys to pass statistical randomness tests as such tests cannot measure entropy, and the number of bits of entropy must be at least equal to the number of bits in the plaintext.
  3. The key must never be reused in whole or in part.
  4. The key must be kept completely secret by the communicating parties.

One-Time Pad

- It is difficult to ensure that the key material is actually random, is used only once, never becomes known to the opposition, and is completely destroyed after use.
  - Some one-time pads were printed on highly flammable nitrocellulose, e.g. flash paper

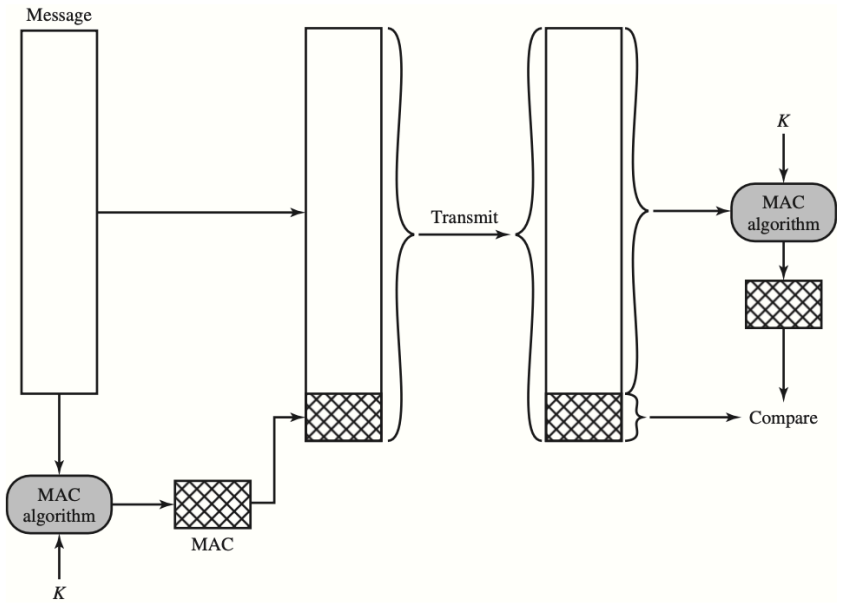
One-Time Pad Example

Message Digest Functions

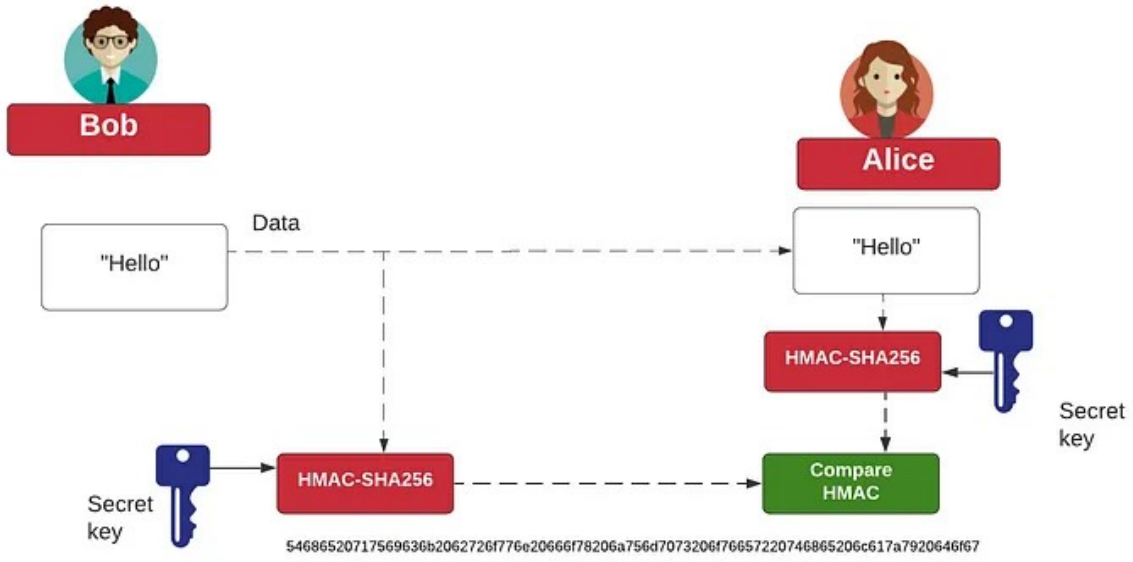
- Encryption protects against passive attack (eavesdropping).
- A different requirement is to protect against active attack (falsification of data and transactions). Protection against such attacks is known as message or data authentication.
  - Verify that the contents of the message have not been altered
  - Verify that the source is authentic.
- Hash and Message Digest functions do not provide Confidentiality
- Confidentiality is provided as a separate function from Integrity / Authenticity.

Message Authentication Code

- Uses a secret key to generate a small block of data, known as a message authentication code, that is appended to the message.



Hash-Based Message Authentication Code



Message Authentication Code

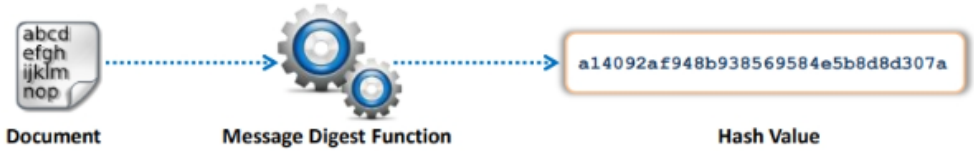
- The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the code, then the receiver's calculation of the code will differ from the received code. Because the attacker is assumed not to know the secret key, the attacker cannot alter the code to correspond to the alterations in the message.

- The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper code.

- If the message includes a sequence number then the receiver can be assured of the proper sequence, because an attacker cannot successfully alter the sequence number.

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.
- Unlike HMAC, hashes don’t require a secret key
- 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

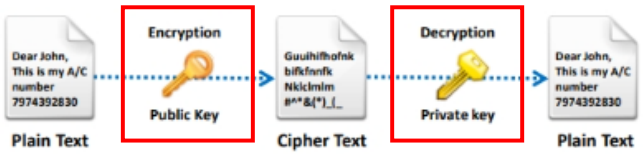


Message Digest (One-Way Hash) Functions

- 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

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.

Requirements for Public Key Cryptography

1. It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).

2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:
   $C = E(PU_b, M)$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext
   using the private key to recover the original message: $M = D(PR_b,C) = D[PR_b, E(PU_b, M)]$

4. It is computationally infeasible for an opponent, knowing the public key, PU_b, to determine the private key, PR_b.

5. It is computationally infeasible for an opponent, knowing the public key, PU_b, and a ciphertext, C, to recover the original message, M.

6. Either of the two related keys can be used for encryption, with the other used for decryption.
   $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$

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

Rivest–Shamir–Adleman (RSA)

RSA works as follows:

- Two large prime numbers are taken (a and b), and their product is determined (c = ab, where “c” is called the modulus).
- RSA chooses a number “e” that it is less than “c” and relatively prime to (a-1)(b-1). Therefore, e and (a-1)(b-1) have no common factor except 1.
- Furthermore, RSA chooses a number “f” such that (ef - 1) is divisible by (a-1)(b-1). 4. The values “e” and “f” are the public and private exponents, respectively.
- The public key is the pair (c, e); the private key is the pair (c, f).
- It is difficult to obtain the private key (c, f) from the public key (c, e). However, if someone can factor “c” into “a” and “b”, then that person can decipher the private key (c, f).

Problems with asymmetric key schemes

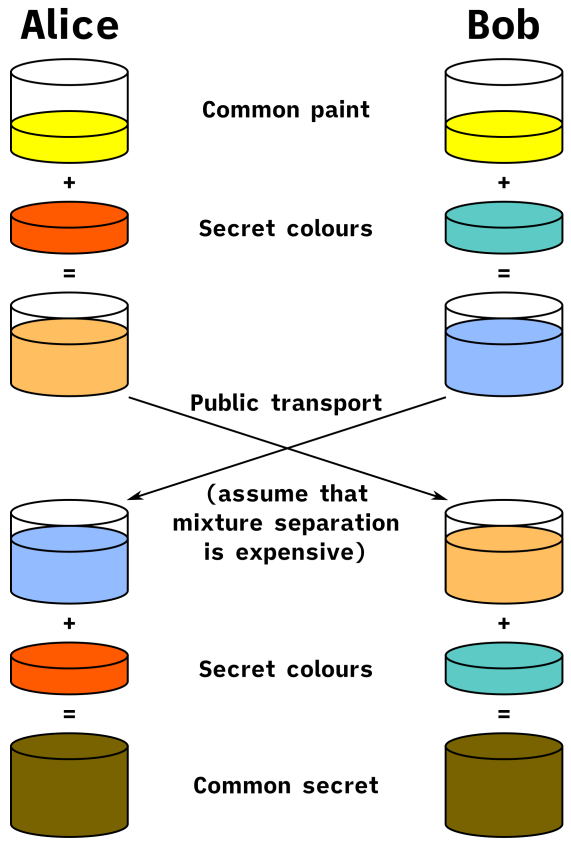
- They are too slow for encrypting internet traffic.
- BUT, symmetric keys have to be pre-shared and a key management nightmare
- But:
  1. How can I symmetrically encrypt my internet traffic with my bank without exchanging keys ahead of time?
  2. How do I know the bank website is actually my bank?

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.



Asymmetric Encryption Applications

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

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.

Digital Signatures

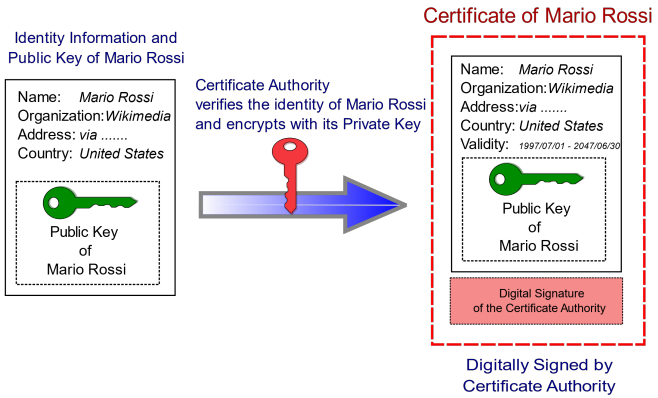
- A digital signature uses asymmetric cryptography and a one-way hash to provide non-repudiation and integrity.
- The document is hashed and the hash is encrypted with the signers private key.
- The recipient hashes the received document. They then decrypt the encrypted hash with the senders public key.
  - 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.

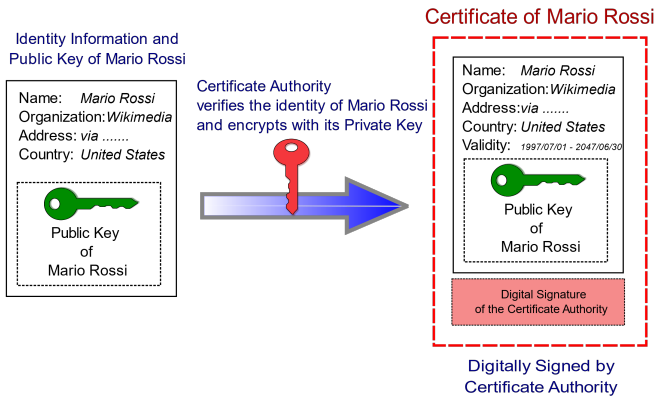
Verifying Website

- 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.