COMPUTER SECURITY

3rd Year Computer Science

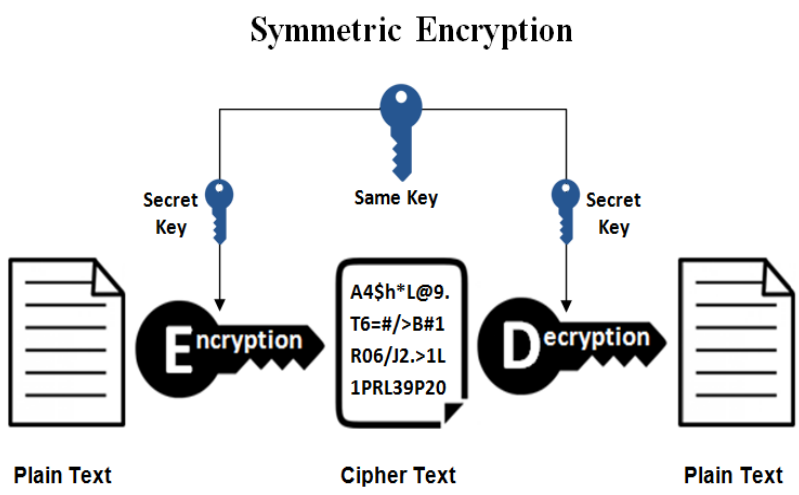
Chapiter 2 :

Introduction to Cryptography

4. Modern Cryptography

- It arose with the advent of computing in the 1960s and the growth of communications systems.
- It is based on machine language (0/1).
- It is applied in the majority of applications: commercial, financial, military, communications, transport, health, etc.

4.1. Symmetric Cryptography (Secret Key)



4.1. Symmetric Cryptography (Secret Key)

Symmetric cryptography uses the same key for both encryption and decryption; this key is usually called **"secret"** because the entire security depends on it being known only by the sender and the recipient.

Symmetric cryptography is widely used and is characterized by high speed (simple operations, on-the-fly encryption) and can be implemented in both software and hardware, greatly increasing throughput.

4.1. Symmetric Cryptography (Secret Key)

There are two types of symmetric encryption:

- **Block encryption:** The encryption operation is performed on blocks of plaintext.
- **Stream encryption (stream cipher):** The encryption operates on each element of the plaintext (character, bit). One bit/character is encrypted at a time.

4.1. Symmetric Cryptography (Secret Key)

Algorithm	Key Size	Assessment
DES (IBM)	56 bits	Too weak today
IDEA (Massey & Xuejia)	128 bits	Effective but patented
RC4 (Ronald Rivest)	1–2048 bits	Some keys are weak
RC5 (Ronald Rivest)	128–256 bits	Effective but patented
AES (Rijndael)	128–256 bits	Best choice
Serpent	128–256 bits	Very strong
Triple DES (IBM)	168 bits	Second best choice
Blowfish (Bruce Schneier)	1–448 bits	Old and slow
Twofish (Bruce Schneier)	128–256 bits	Very strong, widely used

Brief history of block ciphers

- ✦ 1977: DES adopted as a US Federal Information Processing Standard.
- ✦ 1981: DES adopted as a US banking standard.
- ✦ 1988: Triple-DES standardized.
- ✦1997: NIST begins the AES (Advanced Encryption Standard) competition.
- ✦ 1999: 5 finalists for AES announced.
- ✦ 2001: Rijndael adopted for AES.
- ✦ AES has three key lengths: 128, 192 and 256 bits.
- ✦ 2024: No significant weaknesses have been found with AES.
- ✦ AES is ubiquitous, but Triple-DES is still deployed.

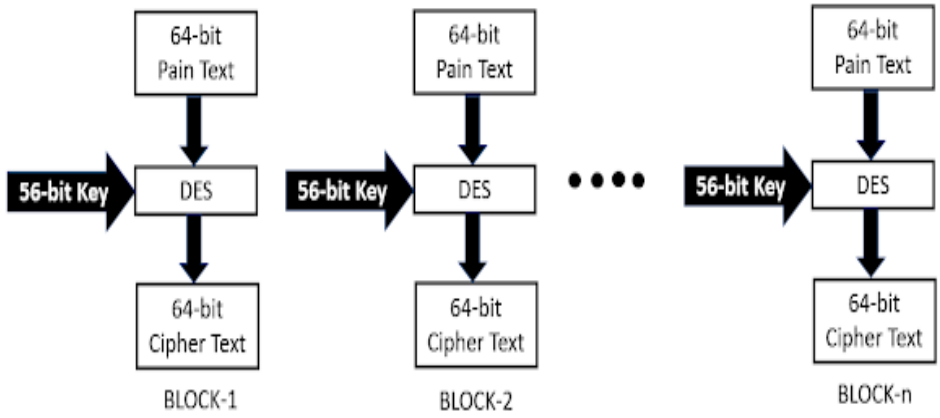
4.1.1. DES (Data Encryption Standard)

Consists of performing combinations, substitutions, and permutations between the text to encrypt and the key. Symmetric block cipher. The key is 64 bits (56 useful + 8 parity bits).

Principle:

1. Split the text into 64-bit (8-byte) blocks;
2. Initial permutation of blocks;
3. Split blocks into two halves: left (L) and right (R);
4. Permutation and substitution steps repeated 16 times (rounds);
5. Reassemble L and R and apply the inverse initial permutation.

4.1.1. DES (Data Encryption Standard)



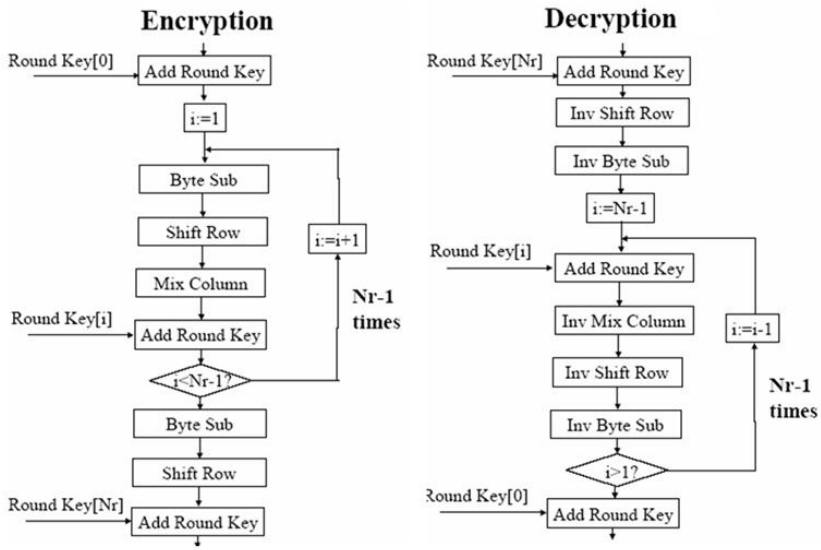
4.1.2. AES (Advanced Encryption Standard)

The increasing power of computers caused the demise of DES. In January 1997, NIST launched an international competition to replace DES, resulting in 15 proposals. In October 2000, NIST selected Rijndael as the new standard, named AES.

Rijndael (named after its designers Rijmen and Daemen) is a block cipher with multiple rounds, similar to DES but with larger and variable block and key sizes: 128, 192, or 256 bits.

Note: AES is a subset of Rijndael; it only works with 128-bit blocks. The difference between AES-128, AES-192, and AES-256 is the key length.

4.1.2. AES (Advanced Encryption Standard)



4.1.2. AES (Advanced Encryption Standard)

Encryption: AES begins with an initial AddRoundKey, then Nr-1 rounds each consisting of:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

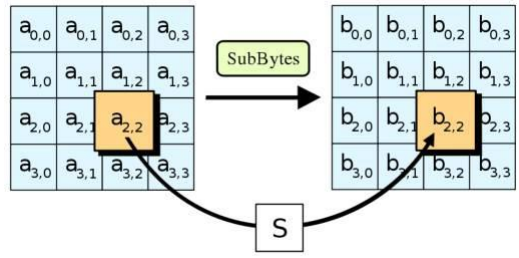
Followed by a final round (FinalRound) omitting MixColumns.

Decryption: The encryption routine is inverted using InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey.

4.1.2. AES (Advanced Encryption Standard)

AES Transformations:

SubByte: All bytes $a_{i,j}$ in the state table are transformed using an invertible S-Box. A single S-Box is sufficient for the entire encryption phase.



4.1.2. AES (Advanced Encryption Standard)

S-Box

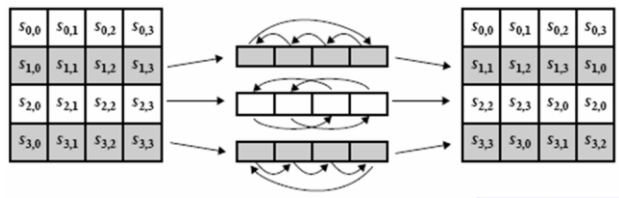
x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

4.1.2. AES (Advanced Encryption Standard)

ShiftRow: Performs a cyclic shift of the rows of the current state table.

Row 0 is never shifted;

rows 1, 2, 3 are shifted by C1, C2, C3 positions respectively.



Shift based on message block size

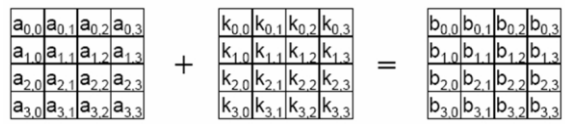
	C_1	C_2	C_3
N_B=4	1	2	3
N_B=6	1	2	3
N_B=8	1	3	4

4.1.2. AES (Advanced Encryption Standard)

MixColumn: Each column of the state is multiplied by a fixed 4×4 matrix.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

AddRoundKey: XOR of the current state with the round key. Adds subkeys to corresponding sub-blocks.

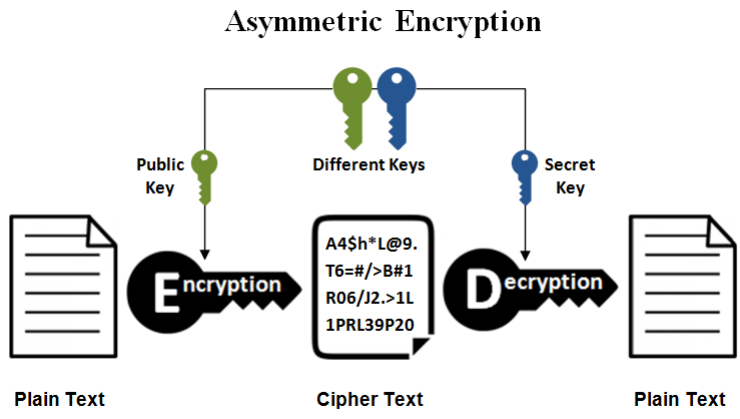


4.1.2. AES (Advanced Encryption Standard)

Advantages of AES:

- Very high performance (more efficient than DES).
- Parallelism can be implemented.
- No arithmetic operations; only shifts and XORs.
- The number of rounds can easily be increased if required.
- It has no weak keys.
- It is resistant to differential and linear cryptanalysis.

4.2. Asymmetric Cryptography (Public Key)



4.2. Asymmetric Cryptography (Public Key)

- In symmetric systems, the same key is used for encryption and decryption. The key distribution problem: for n people to communicate confidentially, n(n-1)/2 keys are needed.
- The concept of public-key cryptosystems was proposed in the foundational 1976 paper by Diffie and Hellman. The fundamental principle is to use different encryption and decryption keys that cannot be derived from each other:

➢ A public key for encryption.

➢ A private key (secret) for decryption.

- This system is based on a one-way function: easy to compute in one direction but very difficult to invert without the private key.

4.2. Asymmetric Cryptography (Public Key)

The big advantage is that there is no need to share a secret in advance to exchange encrypted messages.

The drawback of implementations such as RSA and ElGamal is their slowness compared to symmetric counterparts, which can be up to nearly a thousand times faster.

4.2.1. RSA (Rivest–Shamir–Adleman)

- Proposed in 1978.
- Security depends on the difficulty of factoring large numbers.
- Public key = (n, e) ;
- Private key = (n, d), d computed from p and q (kept secret)

n = p × q (product of two large primes)

- **Encryption:** $y = x^e \bmod n$
- **Decryption:** $x = y^d \bmod n$

4.2.1. RSA (Rivest–Shamir–Adleman)

- **Key generation:**

1. Choose **p** and **q**, two distinct primes.
2. Compute **n = p × q** (the encryption modulus).
3. Compute **φ(n) = (p-1)(q-1)** (Euler's totient).
4. Choose **e**: coprime with f(n) and less than f(n) (encryption exponent).
5. Compute **d**: inverse of **e** modulo **φ(n)**, i.e., $e \times d \equiv 1 \pmod{\varphi(n)}$ (decryption exponent).

4.2.1. RSA (Rivest–Shamir–Adleman)

➢ **Example:**

- Alice chooses p = 17 and q = 19.

  We have: $n = p \times q = 323$, $\varphi(n) = (p-1) \times (q-1) = 288$.

- She chooses e = 5 (for example, and we have GCD(e, φ(n)) = 1).

  We then determine that d = 173 (the modular inverse of e over $Z_{\varphi(n)}$:

  $173 \times 5 = 3 \times 288 + 1$).

  The public key is therefore (5, 323) and the private key is (173, 323).

- Suppose Bob wants to send Alice the message "PRIVATE",
- using the position of each letter in the alphabet to convert them into numbers.

4.2.1. RSA (Rivest–Shamir–Adleman)

➢ **Example:**

- After encrypting by replacing each number P with (P^e mod n), we obtain the message that Bob sends to Alice;
- Alice decrypts by computing C^d mod n = C^{173} mod 323 for each received block, recovering the original values;
- This gives:

Lettre	Position (P)	Cipher (C)
p	16	**118**
r	18	**18**
i	9	**263**
v	22	**167**
a	1	**1**
t	20	**39**
e	5	**218**

4.2.1. RSA (Rivest–Shamir–Adleman)

- **RSA Security:**
- RSA is based on the difficulty of factoring n. Indeed, anyone who manages to factor n can easily recover Alice's secret key knowing only her public key.
- It is not very wise to choose such small values, as d can be recovered very easily. In practice, very large values of p and q must be chosen.

5. Hash Functions

- A hash function is a mathematical function that ensures the integrity of information circulating on the network.
- A hash function computes a short fixed-size fingerprint from an arbitrarily sized input. The result can be called: checksum, fingerprint, hash, message digest, or condensed value.

Example : "Hello“ → H() →185f8db32921bd46d35...

"Hello World with extra text added“ → H() → 78ae647dc5544d227130...

- The probability of two messages having the same hash must be extremely low. The hash does not contain enough information to reconstruct the original text.
- Hash functions are also used for digital signatures.

5. Hash Functions

Properties of hash functions:

- They can be applied to any message length M.
- They produce a fixed-length result.
- It must be easy to compute h = H(M) for any message M.
- For a given h, it is computationally infeasible to find x such that H(x) = h (one-way property).
- For a given x, it is infeasible to find y such that H(y) = H(x) (weak collision resistance).
- It is infeasible to find any x, y such that H(y) = H(x) (strong collision resistance).
- Changing one input bit ideally changes about half the output bits (avalanche effect).

5. Hash Functions

MD5 (Message Digest 5):

Designed by Ronald Rivest (co-creator of RSA), it is one of the most well-known hashing algorithms (successor to MD2 and MD4). Produces a 128-bit digest.

SHA-1 (Secure Hash Algorithm):

Designed by NIST and NSA in 1993, revised in 1995. Produces 160-bit digests. Until 2005 it was the preferred hashing algorithm, but vulnerabilities led to evolution toward more sophisticated versions:

SHA-2, SHA-256, SHA-384, and SHA-512 (the number indicates the digest size in bits).

6. Digital Signatures

- An electronic signature (sometimes called digital signature) is a security mechanism for encrypting a message or document using the sender's private key.
- Like a handwritten signature, it is used to prove the identity of the signer and the integrity of the document.
- A digital signature ensures integrity, authenticity, and non-repudiation of origin.

6. Digital Signatures

Applications of digital signatures:

- Signing and verifying various document formats: Word, Excel, and PDF.
- Performing secure online transactions.
- Identifying participants in an online transaction.
- Verifying digital certificates (e.g. X.509).

6. Digital Signatures

How does a digital signature work?

- To produce a signature, hash functions and public-key encryption are used.
- Signing = hash the message, then encrypt the hash with your private key
- Verifying = decrypt the signature with the sender's public key,
- ecompute the hash, compare
- A digital signature is produced by a digital signature generation algorithm.
- When the recipient receives the message and signature, they verify it using a digital signature verification algorithm.

7. Digital Certificates

A certificate is a digital identity card. It associates a public key with an entity (a server , a person, a machine, ...) to ensure its validity. A certificate is issued by a body called a Certification Authority (CA).

For example, if a browser requests a website, how do we know that the page that's returned to us is the genuine one? Digital certificates provide the stamp of genuineness by binding the public key with the entity (server or client) that owns it, provided the entity possesses the corresponding private key.

7. Digital Certificates

A certificate is a file issued by a CA composed of two parts: one containing information, the other containing the CA's signature. It includes:

- Name, first name, email address + various information
- The person's public key
- Validity date
- Name of the certification authority
- Signature of the certification authority

All this information is signed by the CA: a hash function creates a fingerprint, then this digest is encrypted using the CA's private key. Certificate verification uses the CA's public key and the validity date.

7. Digital Certificates

Types of Digital Certificates

There are three types of Digital Certificates; namely

- TLS/SSL Certificate
- Code Signing Certificate
- Client Certificate

7. Digital Certificates

The certificate structure is standardized by the X.509 standard of the ITU, which defines:

- The X.509 version to which the certificate corresponds
- The certificate serial number
- The encryption algorithm used to sign the certificate
- The name (DN, for Distinguished Name) of the issuing CA
- The certificate start date
- The certificate end date
- The intended use of the public key
- The owner's public key
- The issuer's signature

8. Certification Authorities and PKI

A Public Key Infrastructure (PKI), also called Key Management Infrastructure, is a set of physical components (computers, cryptographic equipment, smart cards), human procedures (verifications, validation), and software (system and application) designed to manage the lifecycle of electronic certificates.

8. Certification Authorities and PKI

A public key infrastructure (PKI) provides a set of services to its users, including:

- User registration (or IT equipment)
- Certificate generation
- Certificate renewal
- Certificate revocation
- Certificate publication
- Publication of revocation lists (CRL)
- Identification and authentication, archiving, escrow, and certificate recovery

Computer security: Introduction to Cryptography

8. Certification Authorities and PKI