Encryption
Block Cipher

Dr.Talal Alkharobi

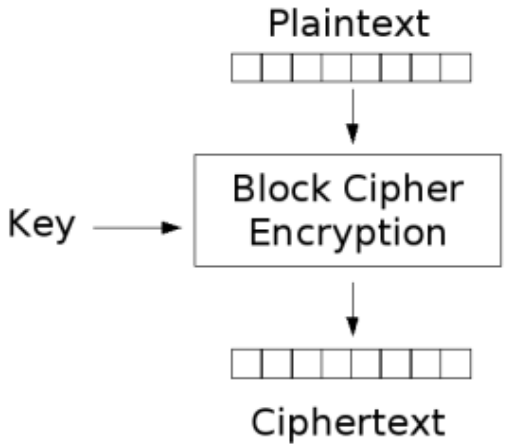
2

Block Cipher

- A symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation.
- When encrypting, a block cipher take n-bit block of plaintext as input, and output a corresponding n-bit block of ciphertext.
- The exact transformation is controlled using a secret key.
- Decryption is similar: the decryption algorithm takes n-bit block of ciphertext together with the secret key, and yields the original n-bit block of plaintext.
- Mode of operation is used to encrypt messages longer than the block size.

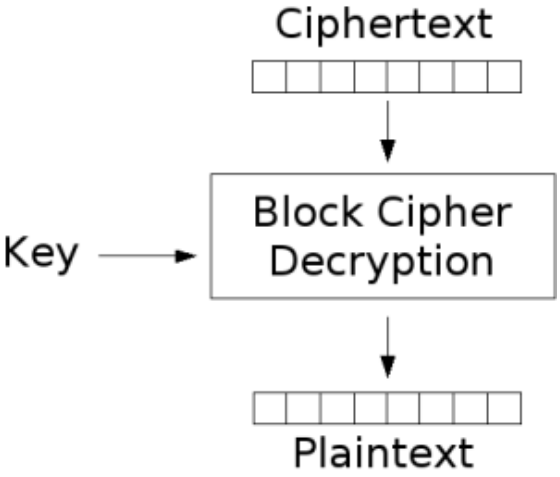
3

Encryption



4

Decryption



5

Block Cipher

- Consists of two algorithms, encryption, *E*, and decryption, *D*.
- Both require two inputs: n-bits block of data and key of size k bits,
- The output is an n-bit block.
- Decryption is the inverse function of encryption:

$$D(E(B,K),K) = B$$

- For each key K, *E* is a permutation over the set of input blocks.
- Each key K selects one permutation from the possible set of $2^n!$.

6

Block Cipher

- The block size, n, is typically 64 or 128 bits, although some ciphers have a variable block size.
- 64 bits was the most common length until the mid-1990s, when new designs began to switch to 128-bit.
- Padding scheme is used to allow plaintexts of arbitrary lengths to be encrypted.
- Typical key sizes (k) include 40, 56, 64, 80, 128, 192 and 256 bits.
- Recently, 80 bits is normally taken as the minimum key length needed to prevent brute force attacks.

7

Iterated block ciphers

- Iterated block ciphers are constructed by repeatedly applying a simpler function.
- Each iteration is termed a round, and the repeated function is termed the round function; anywhere between 4 to 32 rounds are typical.
- Many block ciphers can be categorized as Feistel networks, or, as more general substitution-permutation networks.
- Arithmetic operations, logical operations (especially XOR), S-boxes and various permutations are all frequently used as components.

8

Block Cipher

- Lucifer is generally considered to be the first civilian block cipher, developed at IBM in the 1970s based on work done by Horst Feistel.
- A revised version of the algorithm was adopted as a US government FIPS standard, the Data Encryption Standard (DES).
- It was chosen by the NBS and was publicly released in 1976 and has been widely used.
- As time went on, its inadequacy became apparent, especially after a special purpose machine designed to break DES was demonstrated in 1998 by the Electronic Frontier Foundation.

9

Block Cipher

- A variant of DES, Triple DES, triple-encrypts blocks with (usually) two different keys (2TDES), resulting in a 112-bit keys and 80-bit security.
- It was widely adopted as a replacement and is still (2004) considered secure.
- DES has been superseded as a Federal Standard by the Advanced Encryption Standard (AES), adopted by National Institute of Standards and Technology (NIST) in 2001 after a 5-year public competition.

10

Tweakable block ciphers

- A tweakable block cipher accepts a second input called the tweak along with its usual plaintext or ciphertext input. The tweak, along with the key, selects the permutation computed by the cipher.
- If changing tweaks is sufficiently lightweight (compared with a usually-fairly-expensive key setup operation), then some interesting new operation modes become possible.

Hash functions based on block ciphers

11

- There are several methods to use a block cipher to build a cryptographic hash function.
- The methods resemble the block cipher modes of operation usually used for encryption.
- Using a block cipher as a hash function usually is much slower than using a specially designed hash function.
- However, in some cases, it might be easier since it means just implementing a block cipher and then using it both as a block cipher and a hash function.

Block cipher selected algorithms

12

3-Way | AES | Akelarre | Anubis | ARIA | BaseKing | Blowfish | C2 | Camellia | CAST-128 | CAST-256 | CIKS-1 | CIPHERUNICORN-A | CIPHERUNICORN-E | CMEA | Cobra | COCONUT98 | Crab | CRYPTON | CS-Cipher | DEAL | DES | DES-X | DFC | E2 | FEAL | FROG | G-DES | GOST | Grand Cru | Hasty Pudding Cipher | Hierocrypt | ICE | IDEA | IDEA NXT | Iraqi | Intel Cascade Cipher | KASUMI | KHAZAD | Khufu and Khafre | KN-Cipher | Libelle | LOKI89/91 | LOKI97 | Lucifer | M6 | MacGuffin | Madryga | MAGENTA | MARS | Mercy | MESH | MISTY1 | MMB | MWA | MULTI2 | NewDES | NOEKEON | NUSH | Q | RC2 | RC5 | RC6 | REDOC | Red Pike | S-1 | SAFER | SC2000 | SEED | Serpent | SHACAL | SHARK | Skipjack | SMS4 | Square | TEA | Triple DES | Twofish | UES | Xenon | xmx | XTEA | Zodiac