CSC429 – Computer Security

LECTURE 3
MODERN CRYPTOGRAPHY 2

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Data Encryption Standard (DES)

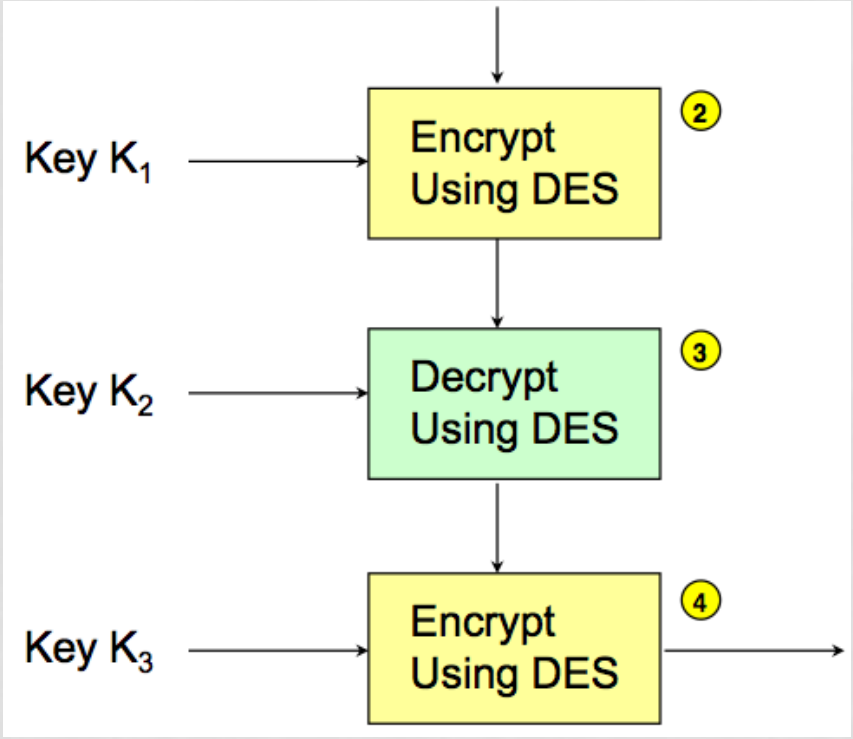
- Designed by IBM, with modifications proposed by the NSA.
- US national standard from 1977 to 2001
- De facto standard
- Block size 64 bits;
- Key size 56 bits
- Designed mostly for hardware implementations
- Considered insecure now
  - vulnerable to brute-force attacks.

Searching for a DES Key

Year	Source	Implemented?	(Estimated) Cost in US$	(Estimated) Search time
1977	Diffie Hellman	No	20 million	20 hours
1993	Wiener	No	10.5 million 1.5 million 600 000	21 minutes 3.5 hours 35 hours
1997	Internet	Yes	Unknown	140 days
1998	Deep Crack	Yes	210 000	56 hours
2007	COPACOBANA	Yes	<10,000	<7 days

Triple DES (3DES)

- Use three different keys
- Key space is 56 x 3 = 168 bits
- No known practical attack against it.



Advanced Encryption Standard (AES)

- In 1997, NIST made a formal call for algorithms stipulating that the AES would specify an unclassified, publicly disclosed encryption algorithm, available royalty-free, worldwide.
- The algorithm must implement symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bits and key sizes of 128-, 192-, and 256-bits.
- In 1998, NIST selected 15 AES candidate algorithms.
- On October 2, 2000, NIST selected **Rijndael** (invented by Joan Daemen and Vincent Rijmen) to as the AES.

Modern Cryptography

Block Ciphers Encryption Modes

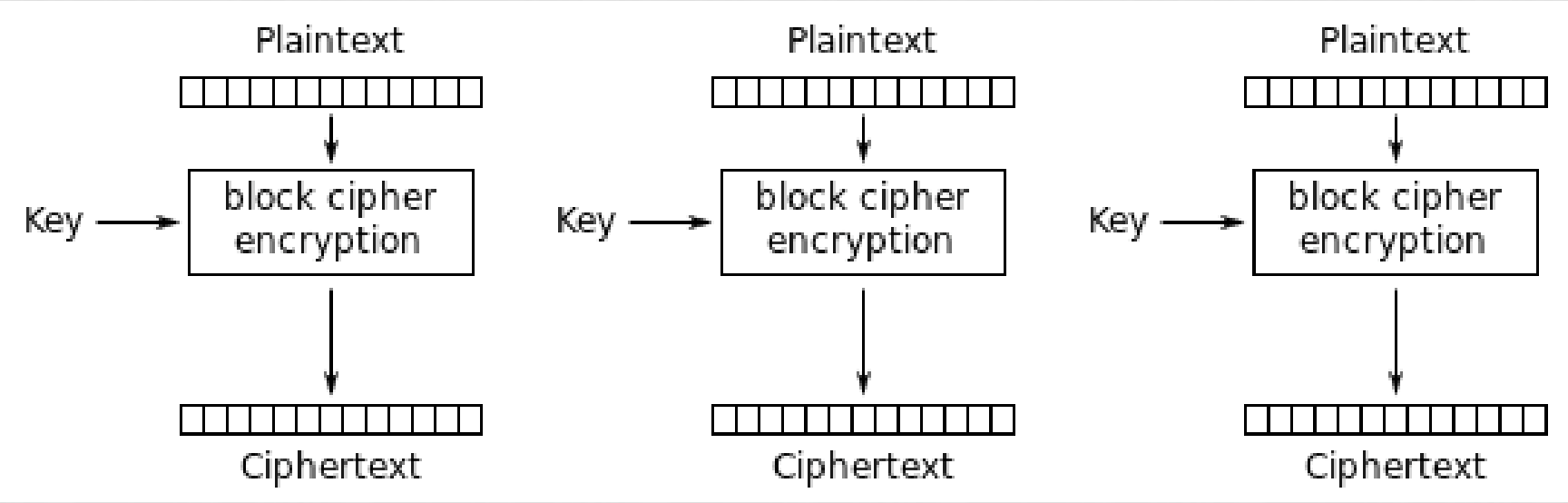
Block Cipher Encryption Modes

- A block cipher encrypts only one block.
- Needs a way to extend it to encrypt an arbitrarily long message.
- Want to ensure that if the block cipher is secure, then the encryption is secure.
- There are many modes: ECB, CBC, CTR, PCBC, CFB, OFB.
  - We will only discuss the first three.

Mode 1 – Electronic Code Book (ECB)

- Message is broken into independent blocks of *block_size* bits;
- Each block encrypted separately.
- **Encryption:** $c_i = E_k(x_i)$
- **Decryption:** $x_i = D_k(c_i)$

ECB Encryption

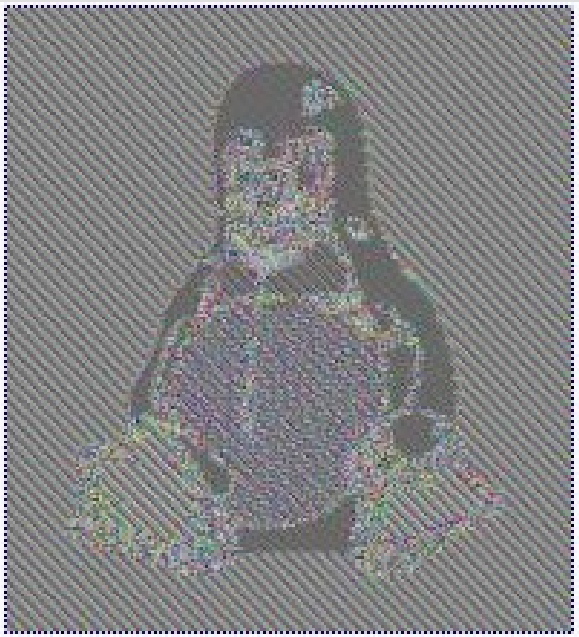


ECB Properties

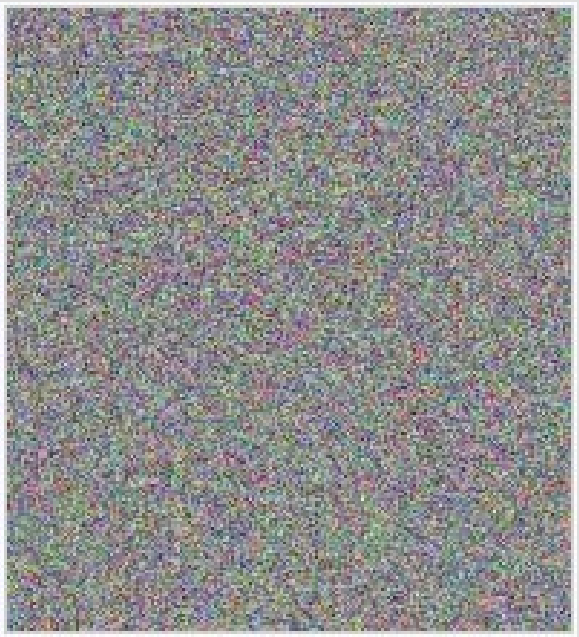
- Deterministic: the same data block gets encrypted the same way, reveals patterns of data when a data block repeats.
- Malleable: reordering ciphertext results in reordered plaintext.
- Errors in one ciphertext block do not propagate.
- Usage: not recommended to encrypt more than one block of data.

ECB vs. Other Modes

Original image



Encrypted using ECB mode

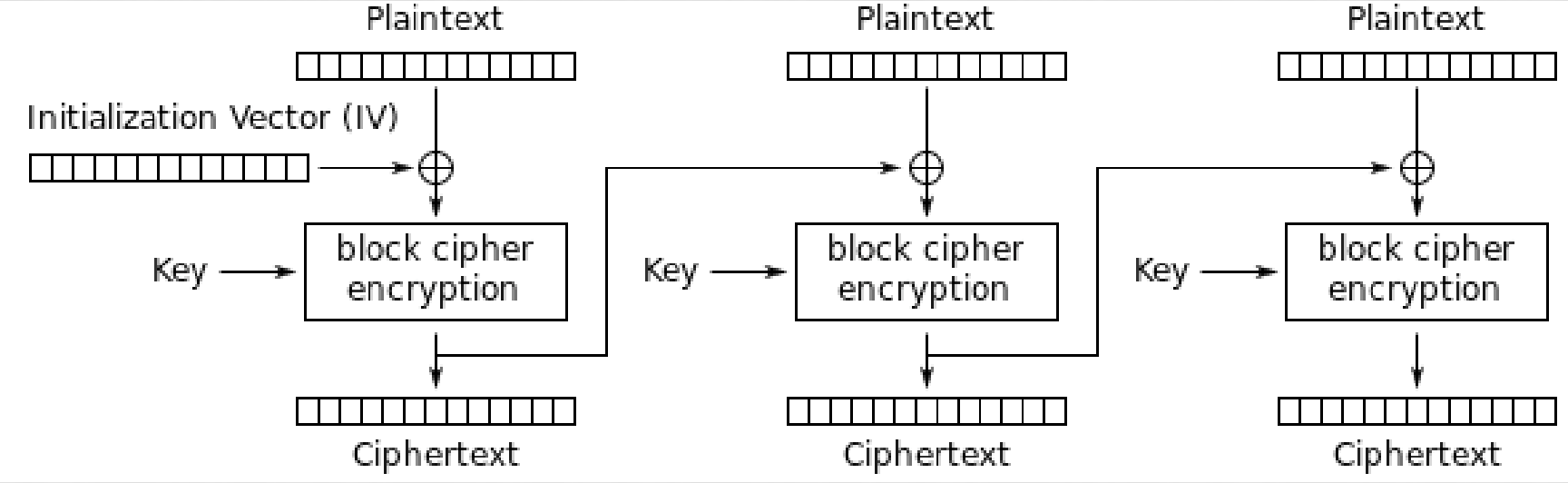


Modes other than ECB result in pseudo-randomness

Mode 2 – Cipher Block Chaining (CBC)

- Next input depends upon previous output
- **Encryption:** $C_i = E_k (M_i \oplus C_{i-1})$, **with** $C_0 = IV$
- **Decryption:** $M_i = C_{i-1} \oplus D_k(C_i)$, **with** $C_0 = IV$

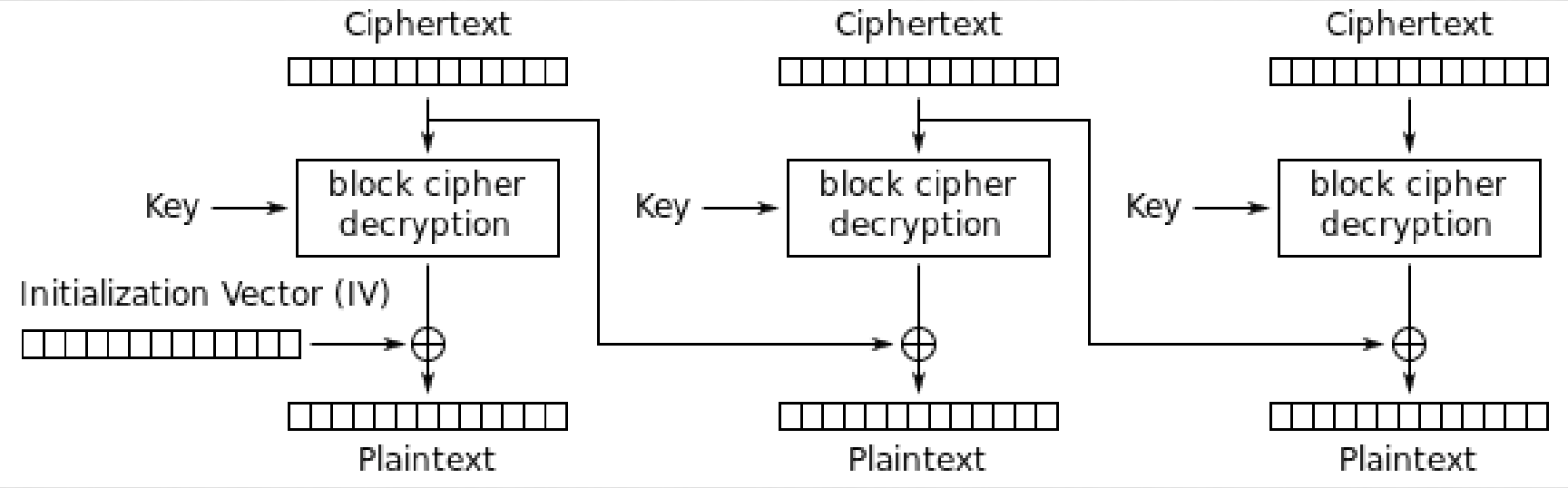
CBC Encryption



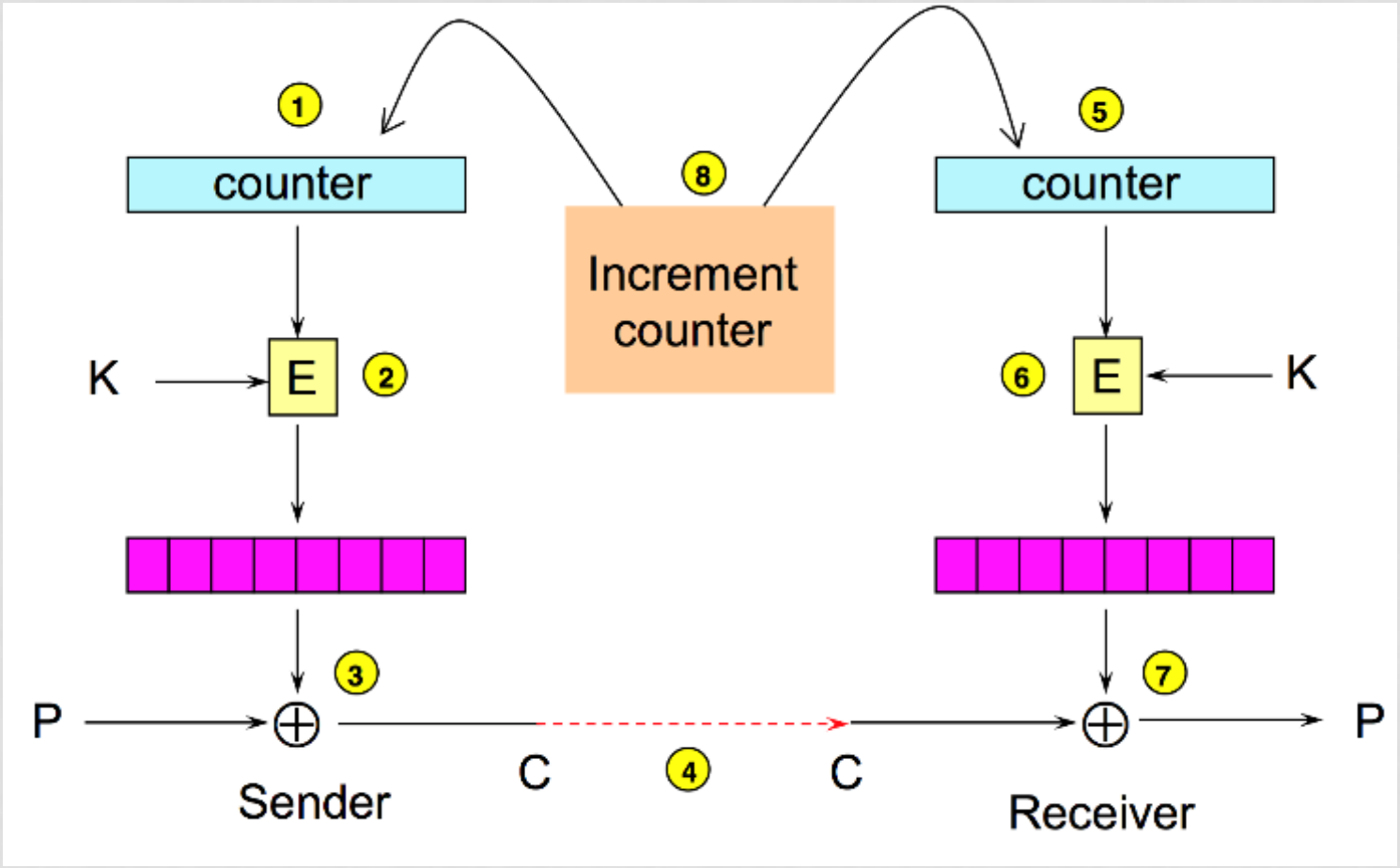
CBC Properties

- Randomized encryption: repeated text gets mapped to different encrypted data.
- A ciphertext block depends on all preceding plaintext blocks; reorder affects decryption.
- Errors in one block propagate to two blocks
  - one bit error in C_j affects all bits in M_j and one bit in M_{j+1}
- Sequential encryption, cannot use parallel hardware.

CBC Decryption



Mode 3 – Counter Mode (CTR)



CTR Mode

- Another way to construct PRNG using a block cipher (e.g. AES):
  - $y_i = E_k[\text{counter}+i]$
- Sender and receiver share: counter (does not need to be secret) and the secret key.

CTR Properties

- Software and hardware efficiency: different blocks can be encrypted in parallel.
- Preprocessing: the encryption part can be done offline and when the message is known, just do the XOR.
- Random access: decryption of a block can be done in random order, very useful for hard-disk encryption.

Breaking Cryptosystems

Attack Scenarios

- Ciphertext-only attack.
- Known-plaintext attack.
- Chosen-plaintext attack.
- Chosen-ciphertext attack.

Breaking a Cryptosystem

- A cryptosystem is usually broken either by:
  - Finding a way of determining the decryption key
  - Finding a way of determining the plaintext directly
- The term "break" is of course subjective.
- Many cryptosystems are "broken" without "breaking" the encryption algorithm.
- Every algorithm can be broken!