

Introduction to Modern Cryptography

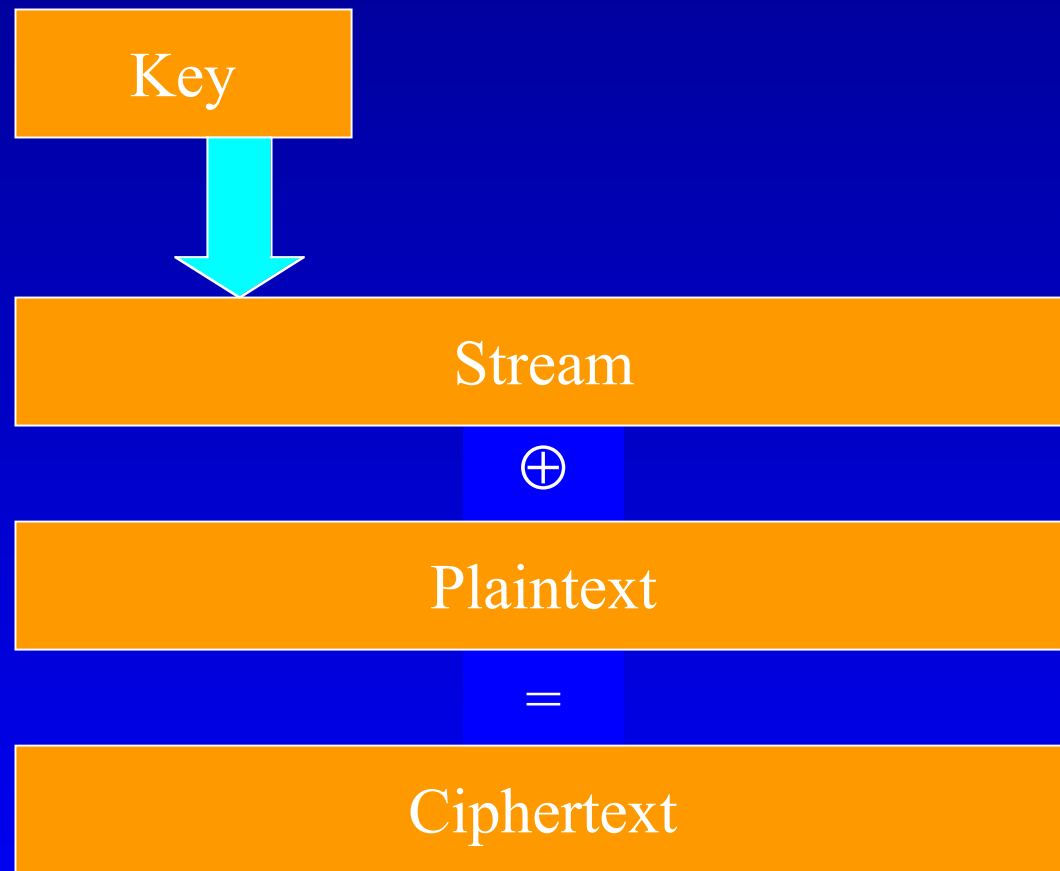
Lecture 2

Symmetric Encryption: Stream & Block Ciphers

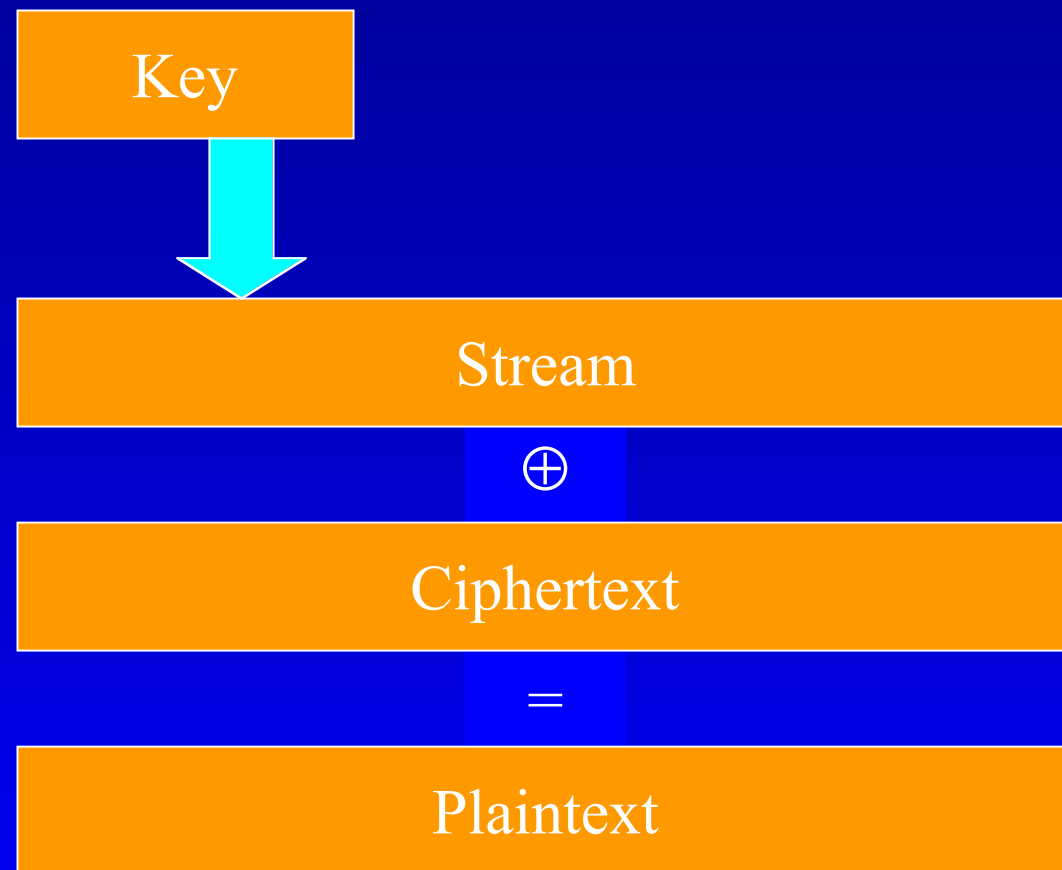
Stream Ciphers

- Start with a secret key (“seed”)
- Generate a **keying stream**
- i -th bit/byte of keying stream is a **function** of the **key** and the first $i-1$ **ciphertext bits**.
- Combine the stream with the plaintext to produce the ciphertext (typically by XOR)

Example of Stream Encryption



Example of Stream Decryption



Real Cipher Streams

- Most pre-WWII machines
- German Enigma
- Linear Feedback Shift Register
- A5 – encrypting GSM handset to base station communication
- RC-4 (Ron's Code)

Terminology

Stream cipher is called **synchronous** if keystream does not depend on the plaintext (depends on key alone).

Otherwise cipher is called **asynchronous**.

Current Example: RC-4

- Part of the RC family
- Claimed by RSA as their IP
- Between 1987 and 1994 its internal was not revealed – little analytic scrutiny
- Preferred export status
- Code released anonymously on the Internet
- Used in many systems: Lotus Notes, SSL, etc.

RC4 Properties

- Variable key size stream cipher with byte oriented operations.
- Based on using a random looking permutation.
- 8-16 machine operations per output byte.
- Very long cipher period (over 10^{100}).
- Widely believed to be secure. Used for encryption in SSL web protocol.

RC-4 Initialization

1. $j=0$
2. $S_0=0, S_1=1, \dots, S_{255}=255$
3. Let the key be k_0, \dots, k_{255} (repeating bits if necessary)
4. For $i=0$ to 255
 - $j = (j + S_i + k_i) \bmod 256$
 - Swap S_i and S_j

RC-4 Key-stream Creation

Generate an output byte B by:

- $i = (i+1) \bmod 256$
- $j = (j + S_i) \bmod 256$
- Swap S_i and S_j
- $t = (S_i + S_j) \bmod 256$
- $B = S_t$

B is XORed with next plaintext byte

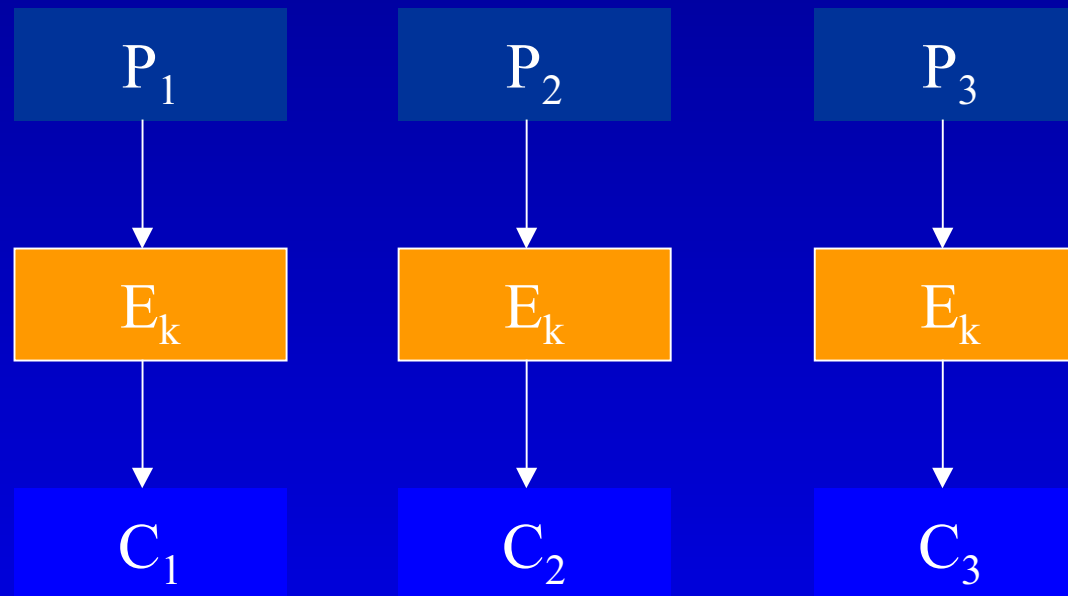
Block Ciphers

- Encrypt a block of input to a block of output
- Typically, the two blocks are of the same length
- Most symmetric key systems block size is 64
- In AES block size is 128
- **Different modes** for encrypting plaintext longer than a block

Real World Block Ciphers

- DES, 3-DES
- **AES** (Rijndael)
- RC-2
- RC-5
- IDEA
- Blowfish, Cast
- Gost

ECB Mode Encryption (Electronic Code Book)



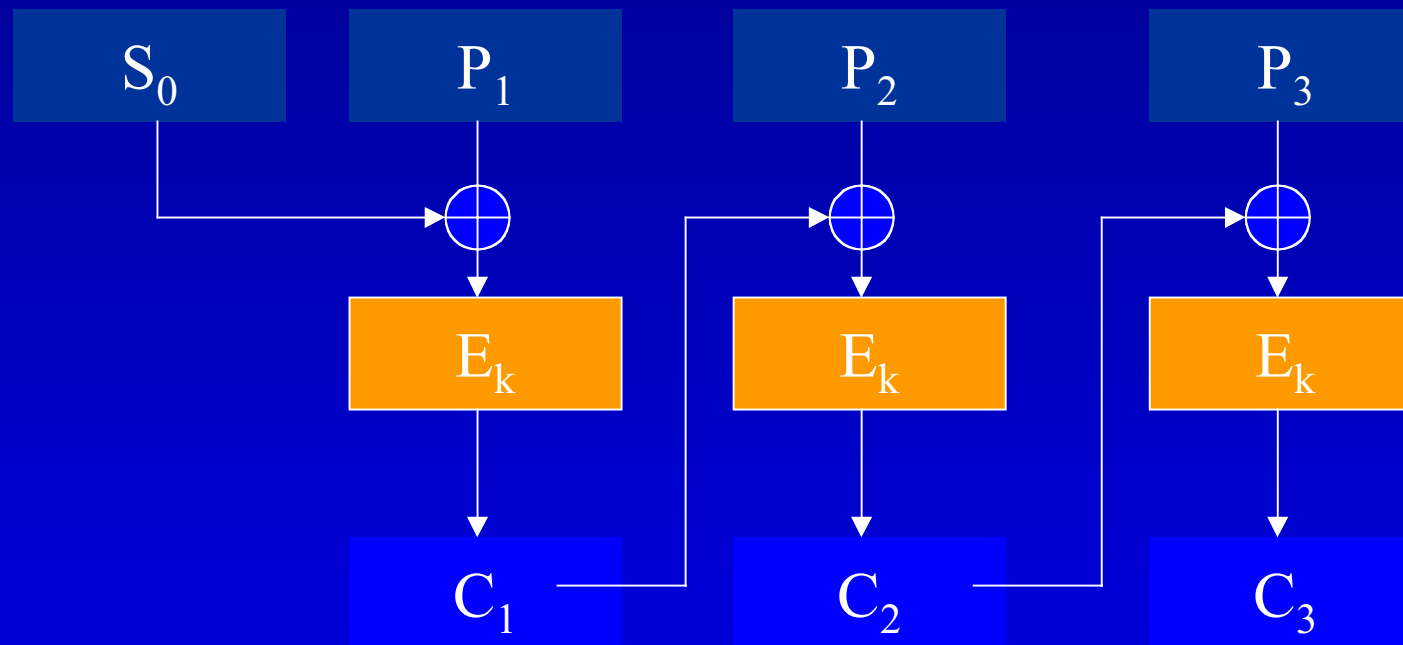
encrypt each plaintext block **separately**

Properties of ECB

- Simple and efficient
- Parallel implementation possible
- Does **not** conceal **plaintext patterns**
- Active attacks are possible (plaintext can be easily manipulated by removing, repeating, or interchanging blocks).



CBC Mode Encryption (Cipher Block Chaining)



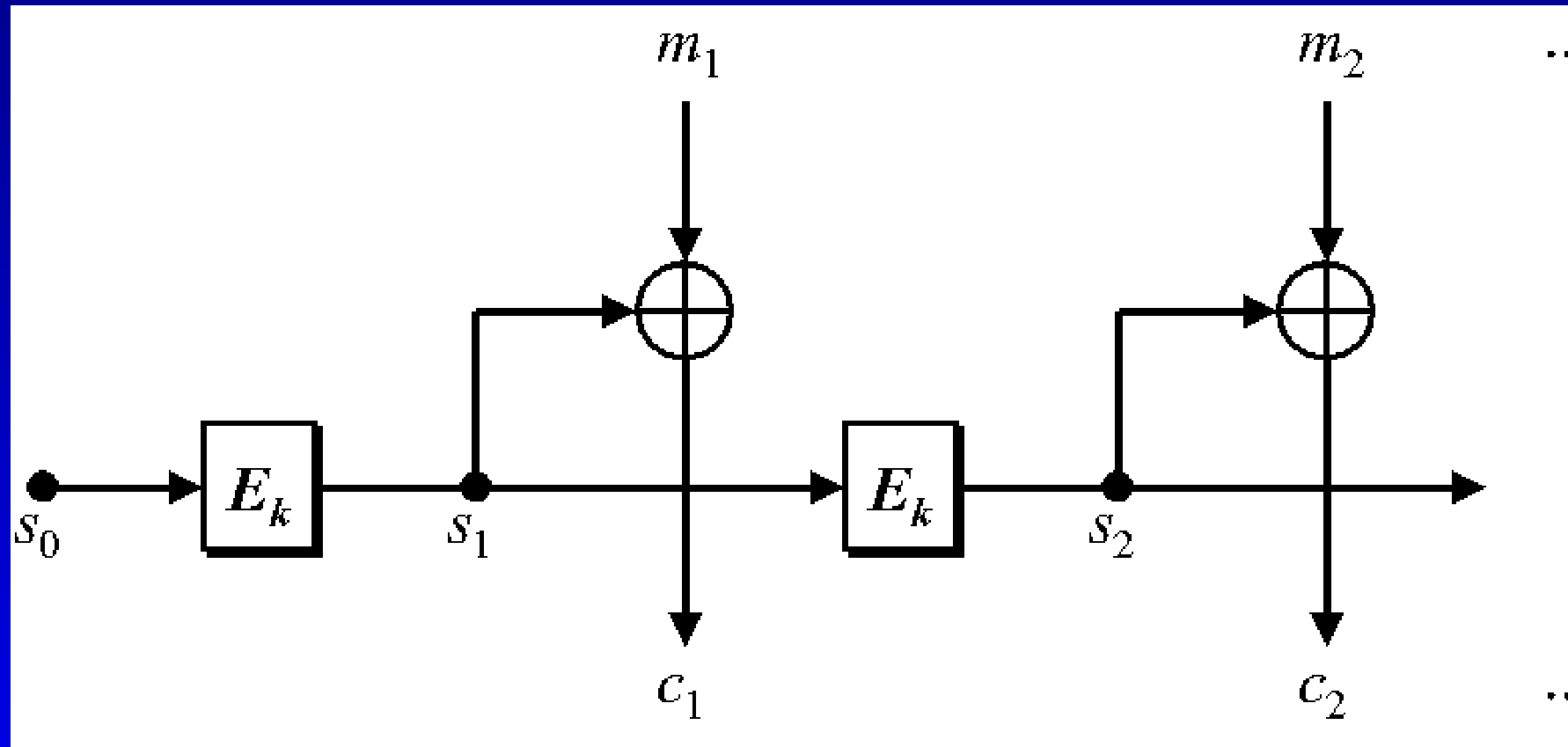
Previous ciphertext is XORed with current plaintext **before** encrypting current block.

An initialization vector S_0 is used as a “seed” for the process.
Seed can be “openly” transmitted.

Properties of CBC

- Asynchronous stream cipher
- Errors in one ciphertext block propagate
- Conceals plaintext patterns
- No parallel implementation known
- Plaintext cannot be easily manipulated.
- Standard in most systems: SSL, IPSec etc.

OFB Mode (Output FeedBack)



An initialization vector s_0 is use as a
``seed'' for a sequence of data blocks s_i

Properties of OFB

- Synchronous stream cipher
- Errors in ciphertext do not propagate
- Pre-processing is possible
- Conceals plaintext patterns
- No parallel implementation known
- Active attacks by manipulating plaintext are possible

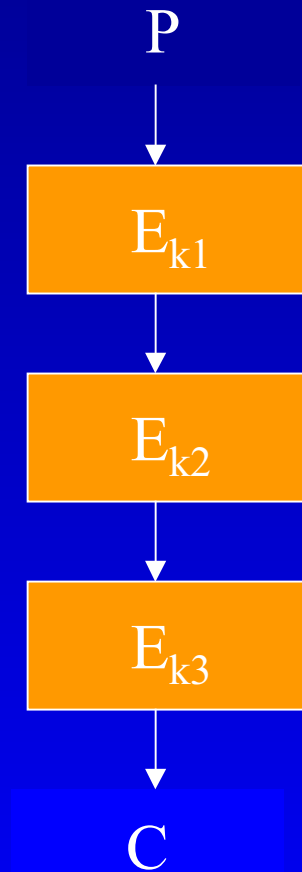
AES Proposed Modes

- CTR (Counter) mode (OFB modification): Parallel implementation, offline pre-processing, provable security, simple and efficient
- OCB (Offset Codebook) mode - parallel implementation, offline preprocessing, provable security (under specific assumptions), authenticity

Strengthening a Given Cipher

- Design multiple key lengths – AES
- Whitening - the DESX idea
- Iterated ciphers – Triple DES (3-DES), triple IDEA and so on

Triple Cipher - Diagram



Iterated Ciphers

- Plaintext undergoes encryption repeatedly by underlying cipher
- Ideally, each stage uses a **different** key
- In practice triple cipher is usually

$C = E_{k_1}(E_{k_2}(E_{k_1}(P)))$ [EEE mode] or

$C = E_{k_1}(D_{k_2}(E_{k_1}(P)))$ [EDE mode]

EDE is more common in practice

Necessary Condition

- For some block ciphers iteration does not enhance security
- Example – substitution cipher
- Consider a block cipher: blocks of size b bits, and key of size k
- The number of all possible **functions** mapping b bits to b bits is $(2^b)^{2^b}$

Necessary Condition (cont.)

- The number of all **possible** encryption functions (**bijections**) is $2^b!$
- The number of encryption functions in our cipher is at most 2^k .
- Claim: The bijections are a group G under the \circ operation (composition)
- Claim: If the encryptions of a cipher form a **sub-group** of G then iterated cipher does **not** increase security.

Meet in the Middle Attack

- Double ciphers are rarely used due to this attack
- Attack requires
 - Known plaintext
 - 2^{k+1} encryptions and decryptions
 - $|k|2^{|k|}$ storage space
- A square root of trivial attacking time at the expense of storage

Meet in the Middle (cont.)

- Given a plaintext-ciphertext pair (p, c)
 - Compute & **store** the table of $D_{k_2}(c)$ for all k_2
takes 2^k decryptions, $|k|2^{|k|}$ storage.
 - For every k_1 , test if $E_{k_1}(p)$ is in table
 - Every hit gives a possible k_1, k_2 pair
 - May have to repeat several times
- Meet in the middle is applicable to any iterated cipher, reducing the trivial processing time by 2^k encryptions

Two or Three Keys

- Sometimes only two keys are used in 3-DES
- Identical key must be at beginning and end
- Legal advantage (export license) due to smaller overall key size
- Used as a KEK in the BPI protocol which secures the DOCSIS cable modem standard

Some Group Theory

Sub-groups

- Let (G, \oplus) be a group. (H, \oplus) is a sub-group of (G, \oplus) if it is a group, and $H \subseteq G$
- Claim: If G is finite and (H, \oplus) is closed, then (H, \oplus) is a sub-group of (G, \oplus) .
- Examples
- Lagrange theorem: if G is finite and (H, \oplus) is a sub-group of (G, \oplus) then $|H|$ divides $|G|$

Order of Elements

- Let a^n denote $a \oplus, \dots, \oplus a$ n times
- We say that a is of order n if $a^n = 1$, and for any $m < n$, $a^m \neq 1$
- Examples
- Euler theorem: in the multiplicative group of Z_n any element is of order at most $\phi(n)$

Adversary's Goals

- Final goal: recover key
- Intermediate goals:
 - Reduce key space
 - Discover plaintext patterns
 - Rec
 - over portions of plaintext
 - Change ciphertext to produce meaningful plaintext, without breaking the system
(active attack)

Generic Attacks

- Exhaustive search
 - Type: ciphertext only
 - Time: $2^{|k|}$ decryptions per ciphertext
 - Storage: constant
- Table lookup
 - Type: chosen plaintext
 - Time: offline $2^{|k|}$ decryptions, online constant
 - Storage: $2^{|k|}$ ciphertexts