Joan Daemen & Vincent Rijmen

CS 553
CRYPTOGRAPHY

Lecture 5
Block Ciphers

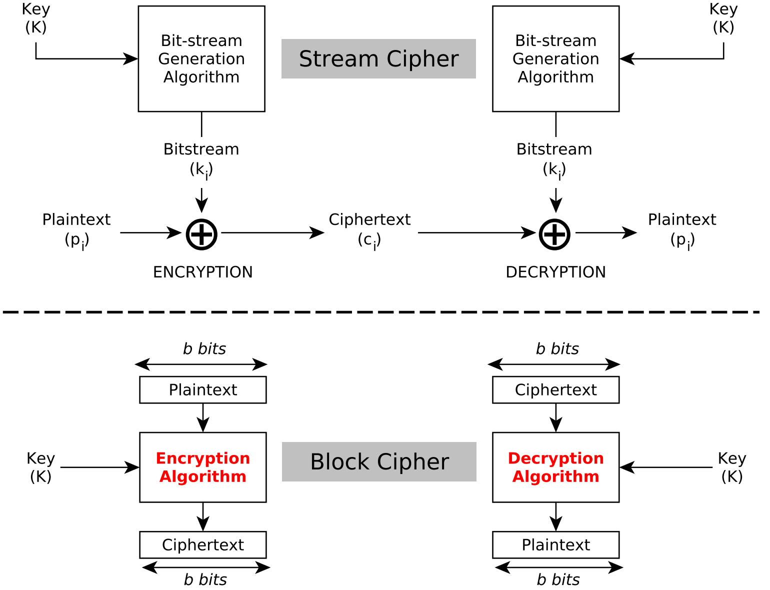
Instructor
Dr. Dhiman Saha

Image Source: Google

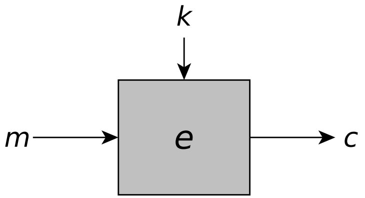
Alice and Bob use the **same** key for Encryption/Decryption

---

http://www.jscape.com/blog/stream-cipher-vs-block-cipher


Key
(K)
Bit-stream Generation Algorithm
Stream Cipher
Bit-stream Generation Algorithm
Key
(K)
Bitstream
(k_i)
Bitstream
(k_i)
Plaintext
(p_i)
Ciphertext
(c_i)
Plaintext
(p_i)
ENCRYPTION
DECRYPTION
b bits
Plaintext
Key
(K)
Encryption Algorithm
Block Cipher
b bits
Ciphertext
Decryption Algorithm
Key
(K)
Ciphertext
b bits
Plaintext
b bits

- Input block m
- Output block c
- Key k
- Block length n



$$e : \{0,1\}^n \times \{0,1\}^{|k|} \to \{0,1\}^n$$

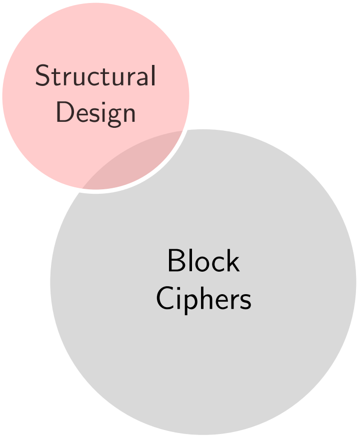
Desired

- Given k easy to encrypt and decrypt: efficiency
- Given m, c hard to compute k, such that $e_k(m) = c$
- One-way property with the key as the inversion trapdoor
- $d(k, e(k, m_0)) = m_0$: deterministic decryption

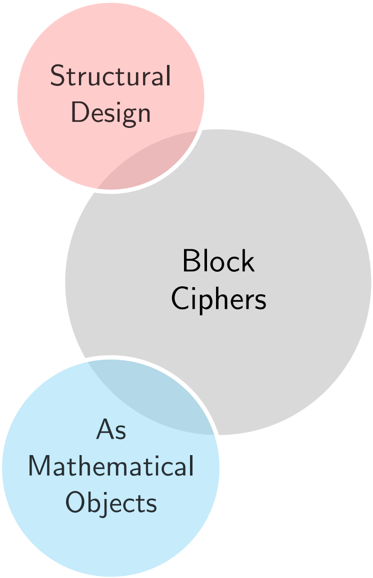
In Today's Talk

Block
Ciphers

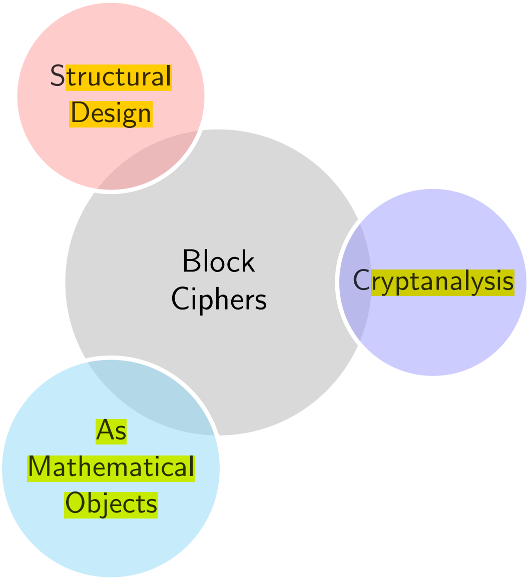
In Today's Talk



In Today's Talk



In Today's Talk



Part I
Inside a Block-Cipher

Is there a rule-of-thumb to design one?

The Structural Aspect

Confusion and Diffusion

- Introduced by Shannon: "*Communication Theory of Secrecy Systems*" 1949 landmark paper
- Still most widely used principles in block cipher design
- Many interpretations: One by Massey

Confusion
: The ciphertext statistics should depend on the plaintext statistics in a manner too complicated to be exploited by the cryptanalyst.

Diffusion
: Each digit of the plaintext and each digit of the secret key should influence many digits of the ciphertext.

Block ciphers are designed to provide sufficient confusion and diffusion.

How to get Confusion and Diffusion?

- Answer comes in the form of two very basic operations

Diffusion

Permutation (P)

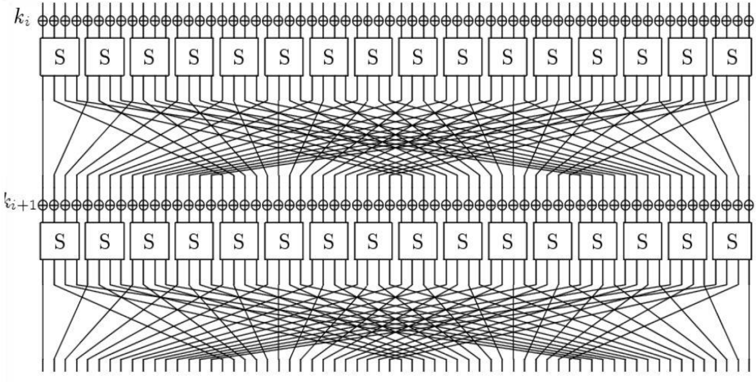
- Bit-level
- Byte-level
- Linear component

Confusion

Substitution (S)

- S-box
- Look-up table
- Non-linear component

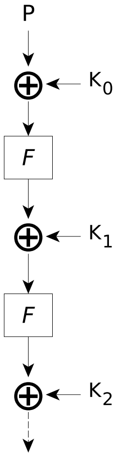
- Block ciphers will contain some combination of S & P
- However, exact form of S & P may vary greatly



x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S[x]$	c	5	6	b	9	0	a	d	3	e	f	8	4	7	1	2

PRESENT Sbox

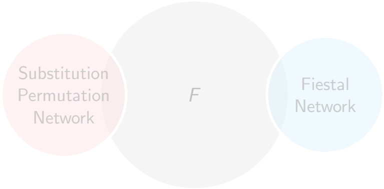
Basic Strategy — Iterate a function



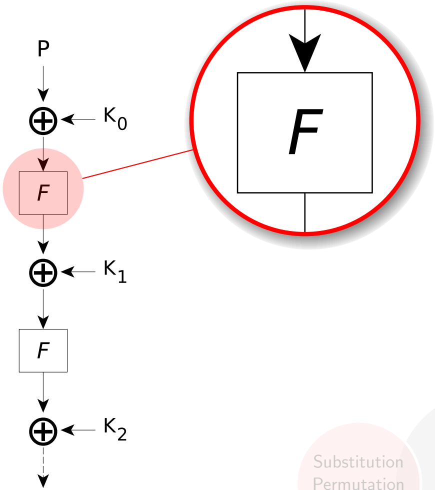
- What is the nature of function F?
- Also known as the **Round Function**
- The design of F lies in the heart of block cipher design

Idea

F itself is weak, but F applied multiple times leads to a secure construction



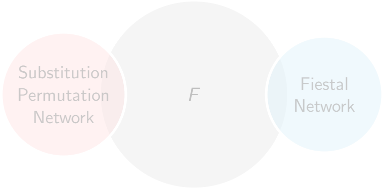
The Round Function



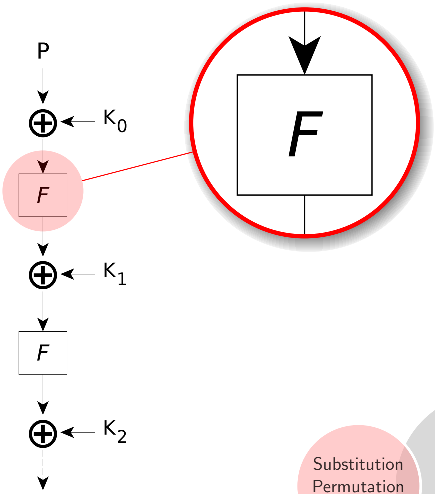
- What is the nature of function F?
- Also known as the **Round** Function
- The design of F lies in the heart of block cipher design

Idea

F itself is weak, but F applied multiple times leads to a secure construction



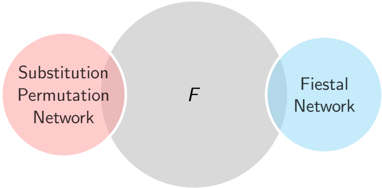
How to design F



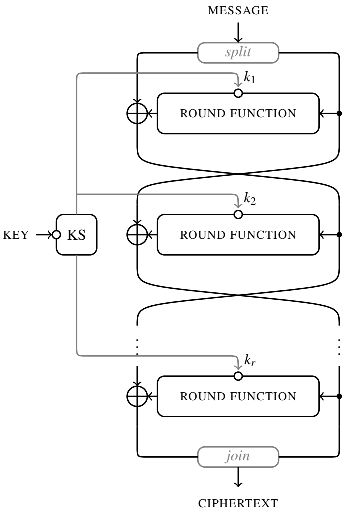
- What is the nature of function F?
- Also known as the **Round Function**
- The design of F lies in the heart of block cipher design

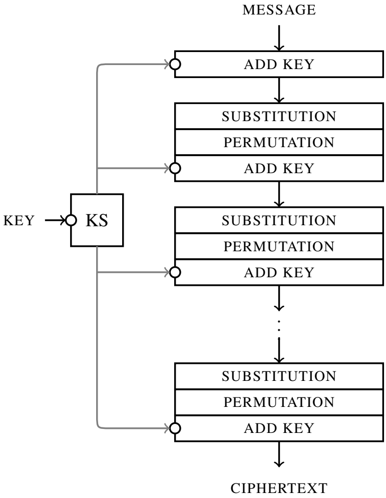
Idea

F itself is weak, but F applied multiple times leads to a secure construction



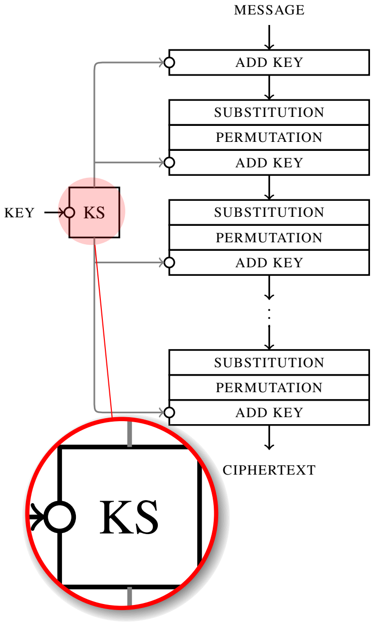
Block Cipher Design Techniques





Fiestal Structure - DES

Classical SPN - AES



Idea

Reusing the key-material intermediately

- The notion of Sub-keys
- Each round-key derived from the user-supplied master-key
- **Key-Scheduling/ Key-Expansion** algorithm
- Some key schedules are computationally lightweight
- Whereas others are very complex.

What if sub-keys are same?

The Slide Attack

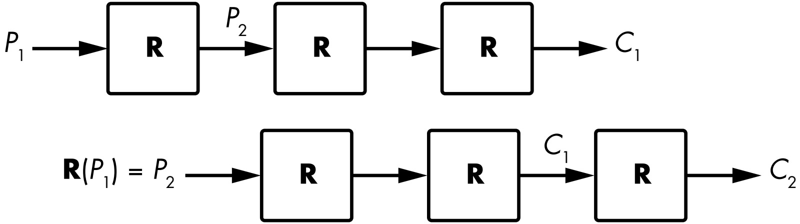
---

https://www.iacr.org/archive/eurocrypt2000/1807/18070595-new.pdf

What if sub-keys are same?

The Slide Attack

When rounds are identical, the relation between the two plaintexts, $P_2 = \mathbf{R}(P_1)$, implies the relation $C_2 = \mathbf{R}(C_1)$



- Note: This is independent of the number of rounds.

https://www.iacr.org/archive/eurocrypt2000/1807/18070595-new.pdf

What if sub-keys are invertible?

- Invertible?
- Meaning we can derive Sub-key-n from Sub-key-$(n+1)$

Implication

If an attacker can recover any round key K_i, he can also recover the main key K

- Typically, usefull for Side-Channel Attacks.

Note

AES Key-schedule is invertible!!!

What we know so far?

- A generic idea of a block cipher
- The iterated structure
- Common design techniques
- But its just processes b-bits at a time

Q: How do we deal with arbitrarily large amount of data?

- Divide and Rule
- Repeatedly instantiate the cipher
- Notion of **Padding**: size must be integral multiple of b

Q: Are the instantiations independent?

Determined by **Mode of Operation**

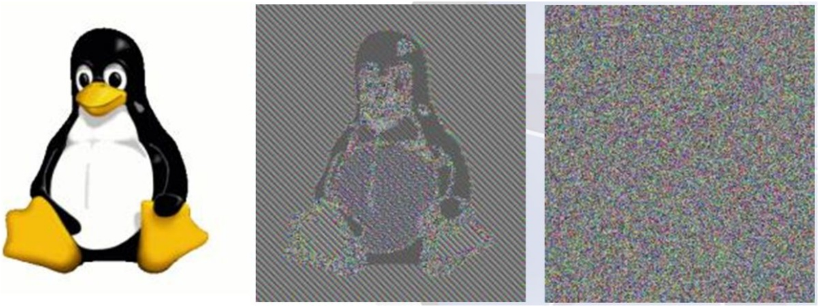
Mode of Operation

The domain-extension algorithm

- Electronic Code Book - EC
- Cipher Block Chaining - CBC
- Output Feedback Mode - OFB
- Cipher Feedback Mode - CFB
- Counter Mode - CTR

Will be discussed in detail later.

Limitation of ECB



Stresses the need for randomization and dependency between instantiations

Image Source: Wikipedia

Part II
Block-Ciphers as Mathematical Objects

What do they represent?

Theoretical Aspect

Block ciphers as family of permutations

- A Block Cipher defines a map that takes plaintexts and keys to ciphertexts.

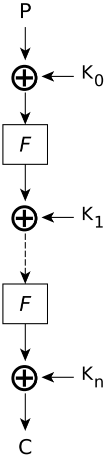
$$\mathcal{E} : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}$$

- fixing a key $K \in \mathcal{K}$ defines a permutation

$$\mathcal{E}_K : \mathcal{P} \rightarrow \mathcal{C}$$

- fixing all keys defines a set

$$E = \{\mathcal{E}_0, \mathcal{E}_1, \cdots, \mathcal{E}_{|\mathcal{K}|-1}\}$$



Thus a block cipher is a way of generating a family of permutations and the family is indexed by a secret key K.

Block ciphers as family of permutations

- A Block Cipher defines a map that takes plaintexts and keys to ciphertexts.

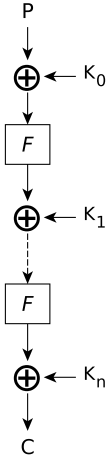
$$\mathcal{E} : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}$$

- fixing a key $K \in \mathcal{K}$ defines a permutation

$$\mathcal{E}_K : \mathcal{P} \rightarrow \mathcal{C}$$

- fixing all keys defines a set

$$E = \{\mathcal{E}_0, \mathcal{E}_1, \cdots, \mathcal{E}_{|\mathcal{K}|-1}\}$$



Thus a block cipher is a way of generating a family of permutations and the family is indexed by a secret key K.

Block cipher, n-bit blocks, k-bit key

- For a given key, a n-bit block cipher maps the set $\mathcal{P}$ of 2^n n-bit inputs onto the same set of 2^n outputs:

$$P = \{\overbrace{0\dots00}^{\text{n}}, \overbrace{0\dots01}^{\text{n}}, \overbrace{0\dots10}^{\text{n}}, \dots, \overbrace{1\dots11}^{\text{n}}\}$$

- The block size n determines the space of all possible permutations that a block cipher might conceivably generate.
  - Number of $n-$bit permutations

$$(2^n)! \approx 2^{(n-1)2^n} \qquad \text{Stirlings approximation}$$

- The key size k determines the number of permutations that are actually generated.
  - Number of $n-$bit permutations generated by block cipher

$$2^k$$

Block cipher, n-bit blocks, k-bit key

- For a given key, a n-bit block cipher maps the set $\mathcal{P}$ of 2^n n-bit inputs onto the same set of 2^n outputs:

$$P = \{\overbrace{0\ldots00}^{\text{n}}, \overbrace{0\ldots01}^{\text{n}}, \overbrace{0\ldots10}^{\text{n}}, \ldots, \overbrace{1\ldots11}^{\text{n}}\}$$

- The block size n determines the space of all possible permutations that a block cipher might conceivably generate.
  - Number of $n-$bit permutations

$(2^n)! \approx 2^{(n-1)2^n}$ Stirlings approximation

- The key size k determines the number of permutations that are actually generated.
  - Number of $n-$bit permutations generated by block cipher

$$2^k$$

The Problem and The Aim

- For typical values of n, k a block cipher provides only a tiny fraction of all the available permutations
- Moreover, it will do so in a highly structured way.

For a good block cipher

A randomly chosen key is expected to "select a permutation seemingly at random from among all $2^{(n-1)2^n}$ possibilities.

- Finally, permutations from related keys should not in turn be related

Design Aim

Choose the 2^k permutations uniformly at random from the set of all $(2^n)!$ permutations

Part III
Block Cipher Cryptanalysis

How to break one?

Modeling the role of Eve

Assumption (Oracle Access)

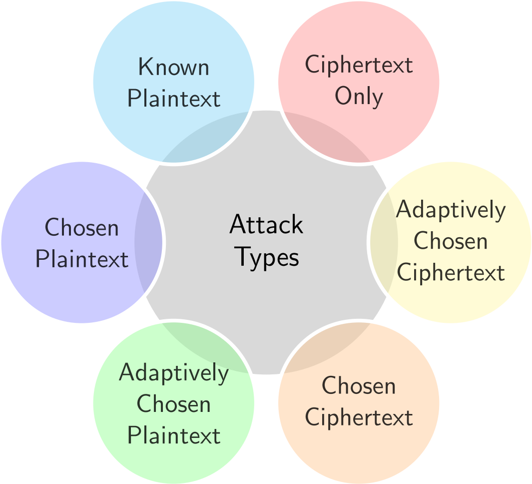
Assume cryptanalyst has access to black-box implementing block cipher with secret key K

Aim of Cryptanalyst

- Find key K, or
- Find (m, c) such that $\mathcal{E}_K(m) = c$ for unknown K, or
- Distinguish member of block cipher from randomly chosen permutation

Classification of Attacks

- Modeling the power of the adversary (Eve)
- Based on the type of data required



Brute-Force → Exhaustive key-search (try all keys, one by one)

A good block cipher is one for which the **best attack** is an exhaustive search.

- Only protection is key-size

k (bits)	Search-time (operations)	Remarks on Security Level (Present Day)
40	2^{40}	Easy to break
64	2^{64}	Practical to break
80	2^{80}	Currently infeasible
128	2^{128}	Very strong
256	2^{256}	Exceptionally strong

Table: Security offered by different key lengths

Specific Attacks

Rely on specific properties of the block-cipher

- Differential Attacks
- Linear Attacks
- Integral Attacks
- Related Key Attacks
- Rebound Attacks
- Boomerang Attacks
- Variants

First Target: **Differential Attacks**