Fundamentals of Information & Network Security
ECE 471/571

Lecture #10: Product Cryptosystems and SPN

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Product Cryptosystems

- Definition: let $S_1 = \{\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1\},\ S_2 = \{\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2\}.$

$$S_1 \times S_2 = \{\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D}\}$$

- Example: a product cipher–Multiplicative Cipher × Shift Cipher
  - It is an Affine cipher!

Idempotent cryptosystems

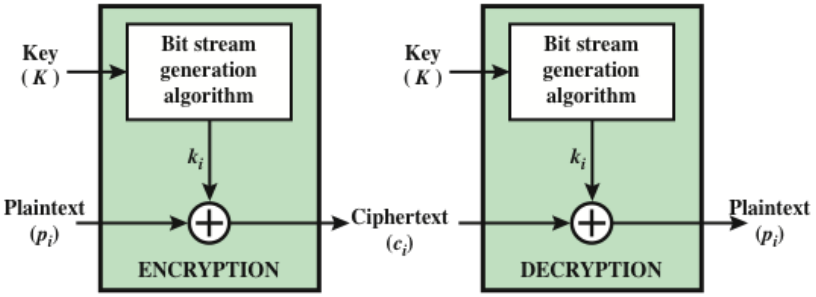
- Idempotent cryptosystems: $S \times S = S$
  - Examples of idempotent cryptosystems?

Does a product of any idempotent cryptosystems has an increased level of security compared to a single encryption system?

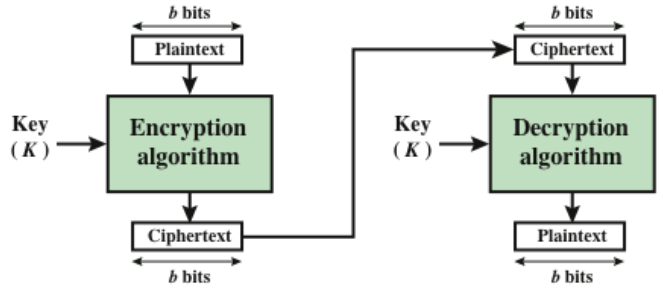
Lemma 1. If two cryptosystems are idempotent and they commute, then the product cryptosystem is also idempotent.

An idempotent cryptosystem does not gain additional security by iterating it
But iterating a nonidempotent cryptosystem does!

Block Ciphers



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Figure 4.1 Stream Cipher and Block Cipher

- Iterative cipher: a block is passed through a number of rounds of encryption according to a key schedule
- Typical Structure

Diffusion and Confusion

- Terms introduced by Claude Shannon to capture the two basic building blocks for any cryptographic system
  - Shannon's concern was to thwart cryptanalysis based on statistical analysis

Diffusion

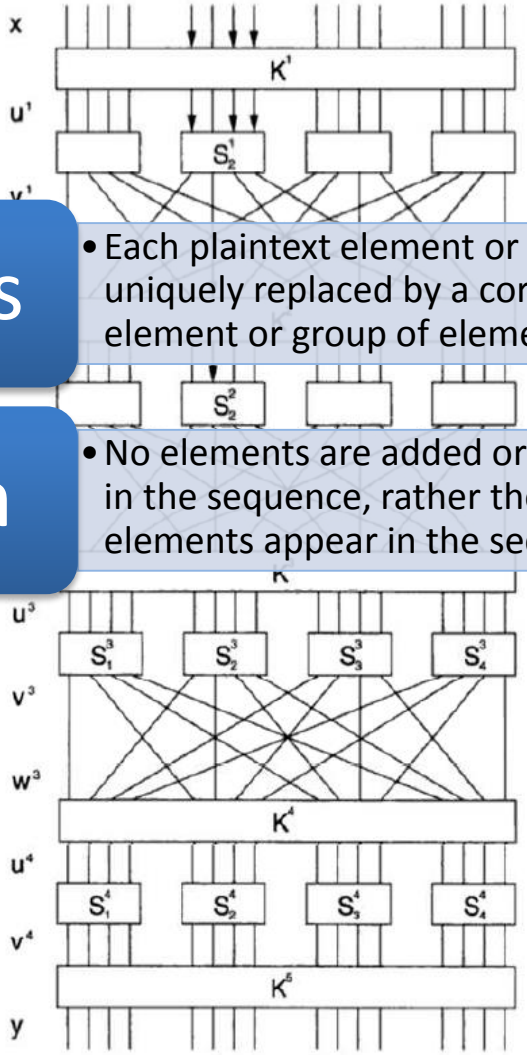
- The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext
- This is achieved by having each plaintext digit affect the value of many ciphertext digits

Confusion

- Seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible
- Even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key

Substitution-Permutation Networks (SPN)

- Idea: Diffusion and Confusion principle from Shannon



Substitutions

- Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements

Permutation

- No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed

Substitution Example

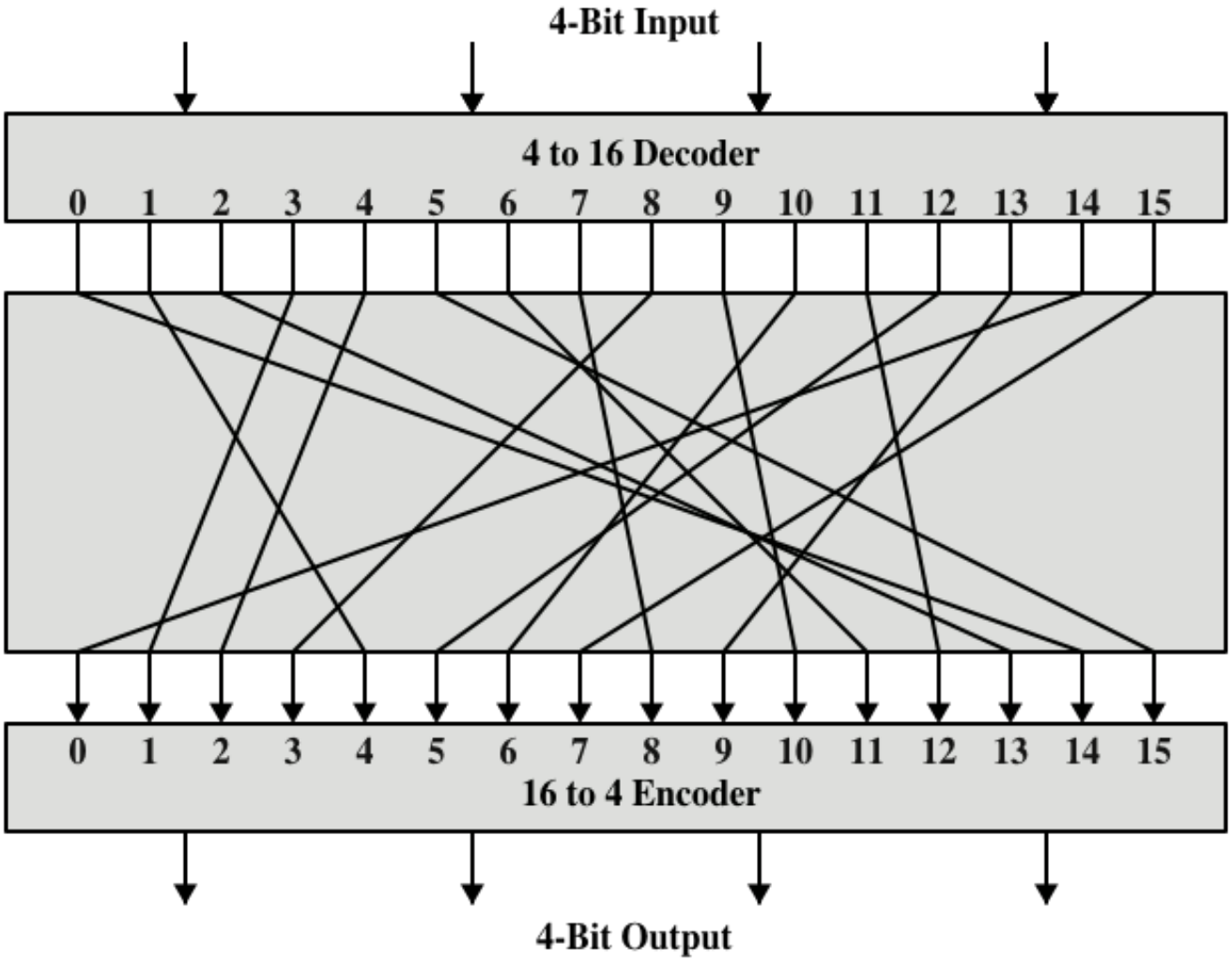


Figure 4.2 General *n*-bit-*n*-bit Block Substitution (shown with $n = 4$)

Encryption and Decryption Tables for Substitution

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Example of SPN

- Activity
  - Assume: $\ell = m = Nr = 4$

π_S

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\pi_S(x)$	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7

π_P

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_p(x)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

  - Let also the key schedule be derived from a 32-bit key K in a cyclic manner by considering 16 consecutive bits beginning from bit k_{4r-3} where r denotes the round. Assume that the initial key is:

    K = 0011 1010 1001 0100 1101 0110 0011 1111

    and the plaintext be x = 0010 0110 1011 0111.
  - Find the ciphertext

Properties of SPN

- S-boxes are very easy to implement in the form of a look-up table.
  - Storage requirement?

- Storage requirement is $\ell 2^{\ell}$, since we have to store 2^ℓ values of length ℓ each. Hence S-boxes have to be small.

- What is the storage requirement for a permutation on ℓ-bits?

Comments

- We could use different S-boxes at each round
- Example not very secure
  - Key space too small: 2^32
- Could improve:
  - Larger key size
  - Larger block length
  - More rounds
  - Larger S-boxes