Aalto University
School of Science

CS-E4320 Cryptography and Data Security
Lecture 3: Block Ciphers

Céline Blondeau

Email: celine dot blondeau at aalto dot fi
Department of Computer Science
Aalto University, School of Science

Fall 2017

Extra information

- Extra lecture on tips for C programming : Thursday 28th at 10:15 in T3
- Slides will be online after the session

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

Outline

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

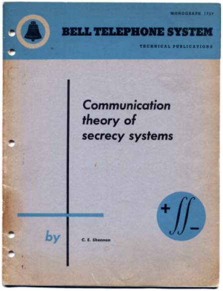
The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

Shannon's bound

- Claude Shannon laid the information theoretic fundamentals of secrecy systems. (USA, 1949)
- Shannon's pessimistic bound: For perfect secrecy, the length of the key is at least that of the plaintext.



MONOGRAPH 1727

BELL TELEPHONE SYSTEM

TECHNICAL PUBLICATIONS

Communication
theory of
secrecy systems

by C. E. Shannon

A note on key length

- The key space $\mathcal{K}$ must be large enough to prevent from exhaustive key search.
- The size of the key space limits the strength of the cryptosystem. The attacker can try all possible keys.
- The length of the key is given in bits. If for the key space $\mathcal{K}$ of the cipher we have

$$|\mathcal{K}| \approx 2^{\kappa} = |\{0,1\}^{\kappa}|$$

  we say that the key length of the cipher is κ bits.
  - The size of the key space of the shift cipher is 26.
    The key length of the shift cipher is $\log_2 26 \approx 4.7$ bits.
  - The number of permutations of $\mathbb{Z}_{26}$ is 26!.
    The size of the key space of the substitution cipher is 26!.
    The key length of the substitution cipher is

$$\log_2 26! = \log_2 403291461126605635584000000 \approx 88.4 \text{ bits.}$$

Diffusion and confusion

Shannon formalized two basic building blocks for a practical cryptosystem.

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

The functional relationship between the ciphertext and the value of the encryption key is as complex as possible. This is achieved by the use of a complex substitution transformation.

Product ciphers

- Shannon formalized the concept of a product cipher: combining two or more transformations in such a way that the resulting cipher is more secure than the individual components.
- product cipher is a practical design for achieving computationally hard problems.
- product cipher is usually composed of layers of
  - small nonlinear substitutions (S-boxes) and
  - affine transformations (including permutations).
- between layers, key is xored to the data like in one-time pad (to be discussed later)
- state-of-the-art ciphers are being designed according to these principles by Shannon

Outline

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

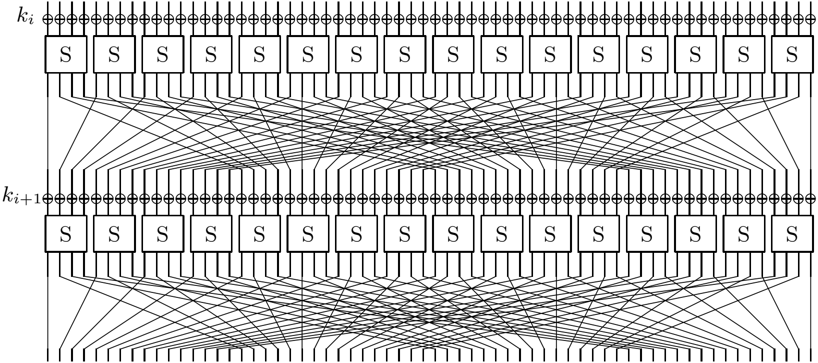
The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

An SPN illustrated

Two rounds of block cipher PRESENT (Bogdanov et al. 2007)


k_i
S S S S S S S S S S S S S S S S
k_{i+1}
S S S S S S S S S S S S S S S S

Substitution permutation networks: definitions

Substitution permutation network (SPN)

Interleave nonlinear substitutions with linear permutations.
Normally bijective.

Substitutions

Input bits go through parallel substitution boxes (S-boxes). These should be chosen according to many strict criteria; intuitively every output bit should depend on every input bit.

Permutations

Output bits go through a permutation box (P-box). This is intuitively chosen s.t. an S-box input comes from many different S-box outputs and, over a number of rounds, each bit affects every other bit.

SPN in practice

- AES
  - NIST Standard since 2002
  - Full description in Lecture 4
- PRESENT
  - Sbox description given in Lecture 2
  - Picture of the round function given in this lecture
  - 31 rounds and 32 key additions
  - Key schedule and full reference: `https://link.springer.com/chapter/10.1007%2F978-3-540-74735-2_31`
  - ISO/IEC 29192-2:2012: standard for lightweight encryption

Outline

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

Feistel networks

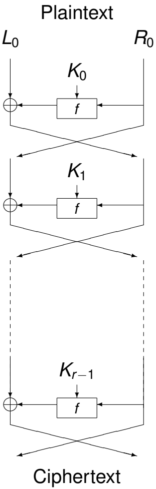
Design

- Select a nonlinear function f.
- Select a key schedule that turns a key K into a series of round keys K_i.
- Split the plaintext into left and right halves L_0 and R_0.
- The output of round i is

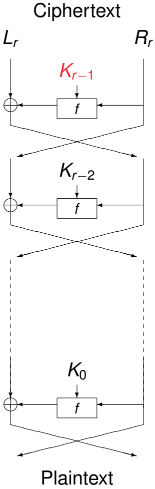
$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus f(R_i, K_i) \end{aligned}$$

Feistel networks: encryption, decryption

Encryption:

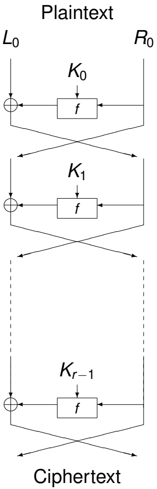


Decryption:

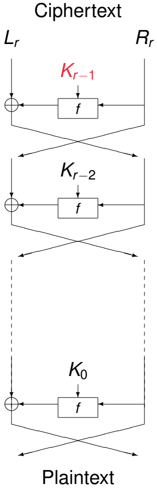


Feistel networks: encryption, decryption

Encryption:



Decryption:



Particularity:

Same function for encryption and decryption, only the order of the round key differ.

f do need not be invertible.

Example: DES

Outline

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

Data Encryption Standard (DES)

Design

The design was a joint effort by NSA and IBM. The design principles were only published little-by-little. The complete set of design criteria is still unknown. Standard for 25 years (1977–2002).

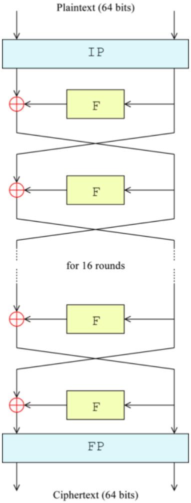
Cryptanalysis

DES has greatly contributed to the development of cryptologic research on block ciphers: differential cryptanalysis (1989), linear cryptanalysis (1993).

Attacks

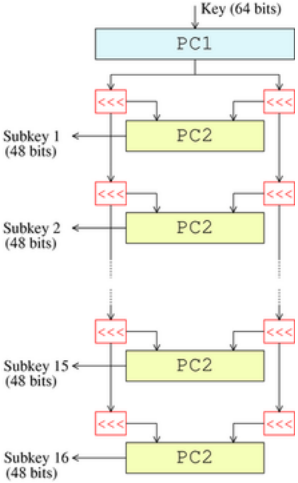
Finally found to be too small. DES key is only 56 bits $\approx 10^{16}$ different keys. Manufacture one million chips where each chip can test one million keys per second, finds the key in about one minute. The EFF DES Cracker (1998) can search for a key in about 4.5 days. The cost of the machine is 250K USD.

DES Feistel structure from Wikipedia



- Feistel cipher, 64-bit blocks, 16 rounds.
- IP and FP are initial and final bit permutations, FP = IP^{-1}.

DES Key Schedule from Wikipedia



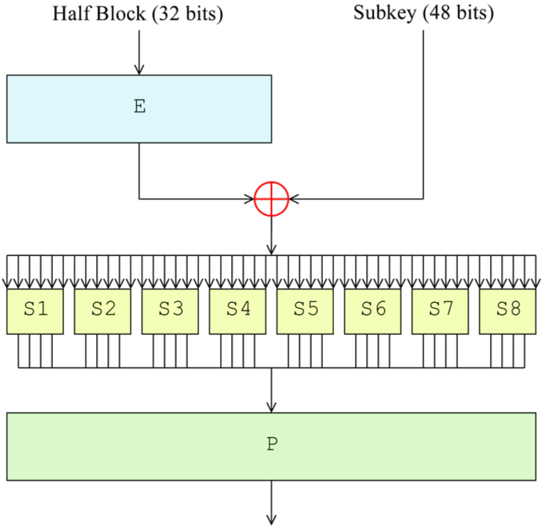
- PC1 and PC2 are permuted selections of bits.
- PC1 selects 56 bits out of the 64 bits.
- PC2 selects 48 bits out of the 2 halves of 28 bits:

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
...					...		
34	53	46	42	50	36	29	32

- First selection of the bit 14. The 48-th bit is the bit 32.
- Concrete key-size : 56 bits.

Aalto University
School of Science

DES round function *F* from Wikipedia



DES round function

- Non-invertible F is an SPN built from eight S-boxes.
- The linear map $E : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{48}$ expands each 4-bit piece to 6-bits by adjoining a single bit from each adjacent piece.
- After the round key addition, the bits in the positions of the two adjoined bits act as the control bits of a 4-to-1 multiplexer: each 6-to-4 bit S-box is composed of 4 bijective 4-to-4 bit S-boxes and the control bits select one of these four small S-box.
- The 4 middle input bits to the S-box is input to the small 4×4 S-box.
- The linear map $P : \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{32}$ simply permutes bits.
- The S-boxes are the only source of nonlinearity in the cipher and have subsequently been the subject of intense study.

Outline

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

A note on attack models

- In a ciphertext only attack the opponent possesses a string of ciphertext y.
- In a known plaintext attack the opponent possesses a string of plaintext x and the corresponding ciphertext y.
- In a chosen plaintext attack the opponent has obtained temporary access to the encryption machine as a *black box* with the unknown key installed. Hence he can choose a plaintext string x and construct the corresponding ciphertext string y.
- In a chosen ciphertext attack the opponent has obtained temporary access to the decryption machine as a black box. Hence he can choose a ciphertext string y and construct the corresponding plaintext string x.

Exhaustive Key Search

- Given (P, C), search all key candidates K_i for a match
$$DES_{K_i}(P) = C.$$
- In general (for all ciphers) this approach gives many false positives if
$$2^{\kappa} = |\mathcal{K}| > |\mathcal{P}| = 2^n.$$
- Given one pair (P, C) the probability that a wrong key passes the test is
$$\Pr(\ K_i \text{ passes }) \approx 2^{-n}.$$
- Given t pairs $(P_1, C_1), \ldots, (P_t, C_t)$ the probability of false positives is
$$\Pr(K_i \text{ passes }) \approx 2^{-tn}.$$
- The average number (taken over P) of false positives is $2^{\kappa - tn}$ block size

Outline

Shannon Theory

Substitution Permutation Networks

Feistel Ciphers

The DES

Attack Models and Exhaustive Key Search

Meet-in-the Middle Attack and Triple DES

Double Encryption

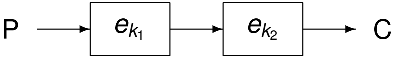
P: Plaintext
C: Ciphertext
DES: $\ell = 56$

- e_k: block cipher
- k: key of length ℓ bits
- d_k: decryption function

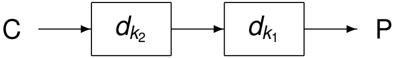
- Double encryption:

$$C = E_K(P) = e_{k_2}(e_{k_1}(P)),$$

with a key $K = (k_1, k_2)$ of length 2ℓ bits



- Decryption:



Double Encryption

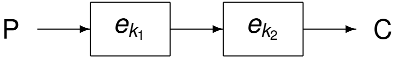
P: Plaintext
C: Ciphertext
DES: $\ell = 56$

- e_k: block cipher
- k: key of length ℓ bits
- d_k: decryption function

- Double encryption:

$$C = E_K(P) = e_{k_2}(e_{k_1}(P)),$$

with a key $K = (k_1, k_2)$ of length 2ℓ bits



-

- What is the “a priori” security level of the double encryption?

Double Encryption

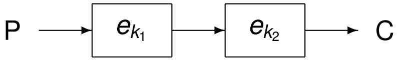
P: Plaintext
C: Ciphertext

DES: $\ell = 56$

- e_k: block cipher
- k: key of length ℓ bits
- d_k: decryption function
- Double encryption:

$$C = E_K(P) = e_{k_2}(e_{k_1}(P)),$$

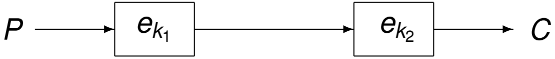
with a key $K = (k_1, k_2)$ of length 2ℓ bits



-
- What is the “a priori” security level of the double encryption?
- 2ℓ bits (112 bits for the double DES)

Meet in the Middle Attack on Double Encryption

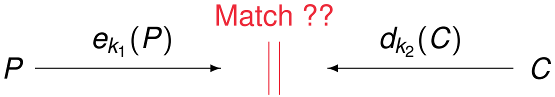
- Double encryption: $C = e_{k_2}(e_{k_1}(P))$



P e_{k_1} e_{k_2} C

- Observation: $e_{k_1}(P) = d_{k_2}(C)$

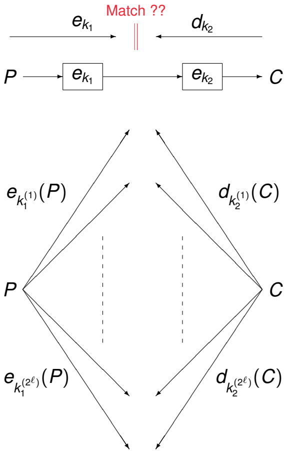
- Meet in the Middle (MitM) attack, basic idea:
  - Find two keys k_1 and k_2 for which $e_{k_1}(P) = d_{k_2}(C)$



Match ??

P $e_{k_1}(P)$ $d_{k_2}(C)$ C

Meet in the Middle Attack: Algorithm



Meet in the Middle (MitM) Attack:

- Given a plaintext-ciphertext pair (P, C)
- Build a hash table T where $T[E_{k_1^{(i)}}(P)] = k_1^{(i)}$
- For all $k_2^{(j)}$
    - Compute $d_{k_2^{(j)}}(C)$
    - If $d_{k_2^{(j)}}(C)$ is in T
        - $(k_1^{(i)}, k_2^{(j)})$ is a potential candidate
        - Check with other pairs (P', C'), (P'', C''), $\cdots$

MitM Attack: Complexity

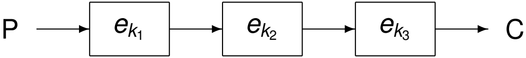
Time: $\mathcal{O}(2^\ell)$
Memory: $\mathcal{O}(1)$

- Time complexity: $\mathcal{O}(2^{\ell+1})$
  - 2^ℓ encryptions and 2^ℓ decryptions
- Memory complexity: $\mathcal{O}(2^\ell)$
  - Storage of the hash table
- The security level of the double encryption cipher with a key of length 2ℓ bits is reduced to $\ell + 1$ bits

Triple Encryption

Triple encryption:

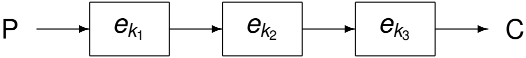
- Given $K = (k_1, k_2, k_3)$, $C = E_K(P) = e_{k_3}(e_{k_2}(e_{k_1}(P)))$



Triple Encryption

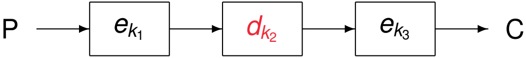
Triple encryption:

- Given $K = (k_1, k_2, k_3)$, $C = E_K(P) = e_{k_3}(e_{k_2}(e_{k_1}(P)))$



Encryption, decryption, encryption (EDE):

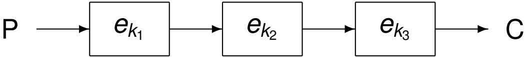
- $C = E_K(P) = e_{k_3}(d_{k_2}(e_{k_1}(P)))$



Triple Encryption

Triple encryption:

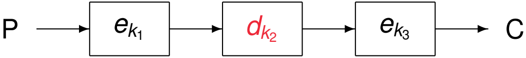
- Given $K = (k_1, k_2, k_3)$, $C = E_K(P) = e_{k_3}(e_{k_2}(e_{k_1}(P)))$



P e_{k_1} e_{k_2} e_{k_3} C

Encryption, decryption, encryption (EDE):

- $C = E_K(P) = e_{k_3}(d_{k_2}(e_{k_1}(P)))$



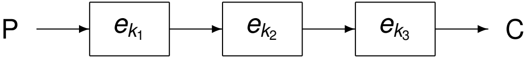
P e_{k_1} d_{k_2} e_{k_3} C

What happens to the EDE cipher if $k_2 = k_1$ (or $k_3 = k_2$)?

Triple Encryption

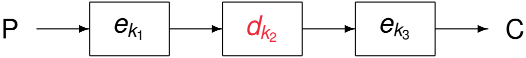
Triple encryption:

- Given $K = (k_1, k_2, k_3)$, $C = E_K(P) = e_{k_3}(e_{k_2}(e_{k_1}(P)))$



Encryption, decryption, encryption (EDE):

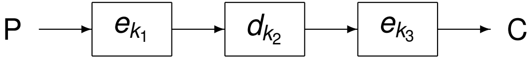
- $C = E_K(P) = e_{k_3}(d_{k_2}(e_{k_1}(P)))$



What happens to the EDE cipher if $k_2 = k_1$ (or $k_3 = k_2$)?

- $C = e_{k_3}(P)$ (or $C = e_{k_1}(P)$)

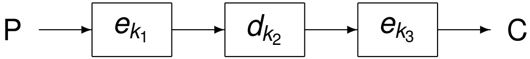
Triple DES



Triple DES (TDES or TDEA or 3DES):

- Encrypts blocks of 64 bits
- EDE procedure with $e_k = DES_k$
- 3 keying options
- Keying Option 1: k_1, k_2, and k_3 are 3 independent 56-bit keys
- Keying Option 2: k_1 and k_2 are independent, $k_3 = k_1$
- Keying Option 3: $k_1 = k_2 = k_3$

Triple DES



Triple DES (TDES or TDEA or 3DES):

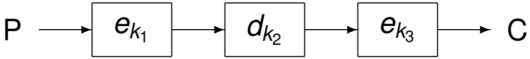
- Encrypts blocks of 64 bits
- EDE procedure with $e_k = DES_k$
- 3 keying options

- Keying Option 1: k_1, k_2, and k_3 are 3 independent 56-bit keys

- Keying Option 2: k_1 and k_2 are independent, $k_3 = k_1$

- Keying Option 3: $k_1 = k_2 = k_3$
  - Simple DES

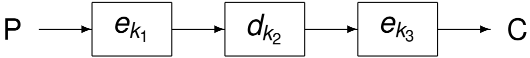
Triple DES



Triple DES (TDES or TDEA or 3DES):

- Encrypts blocks of 64 bits
- EDE procedure with $e_k = DES_k$
- 3 keying options
- Keying Option 1: k_1, k_2, and k_3 are 3 independent 56-bit keys
- Keying Option 2: k_1 and k_2 are independent, $k_3 = k_1$
  - Exhaustive key search: Time $\mathcal{O}(2^{112})$, Memory $\mathcal{O}(1)$
- Keying Option 3: $k_1 = k_2 = k_3$
  - Simple DES

Triple DES



Triple DES (TDES or TDEA or 3DES):

- Encrypts blocks of 64 bits
- EDE procedure with $e_k = DES_k$
- 3 keying options

- Keying Option 1: k_1, k_2, and k_3 are 3 independent 56-bit keys
  - MitM attack: Time $\mathcal{O}(2^{112})$, Memory $\mathcal{O}(2^{56})$
- Keying Option 2: k_1 and k_2 are independent, $k_3 = k_1$
  - Exhaustive key search: Time $\mathcal{O}(2^{112})$, Memory $\mathcal{O}(1)$
- Keying Option 3: $k_1 = k_2 = k_3$
  - Simple DES

Supplemental reading

Understanding cryptography

Section 3.3–7
Section 5.3
Section 5.1-5.3

Handbook of applied cryptography

Section 7.4.2–3
Section 7.2.1–3