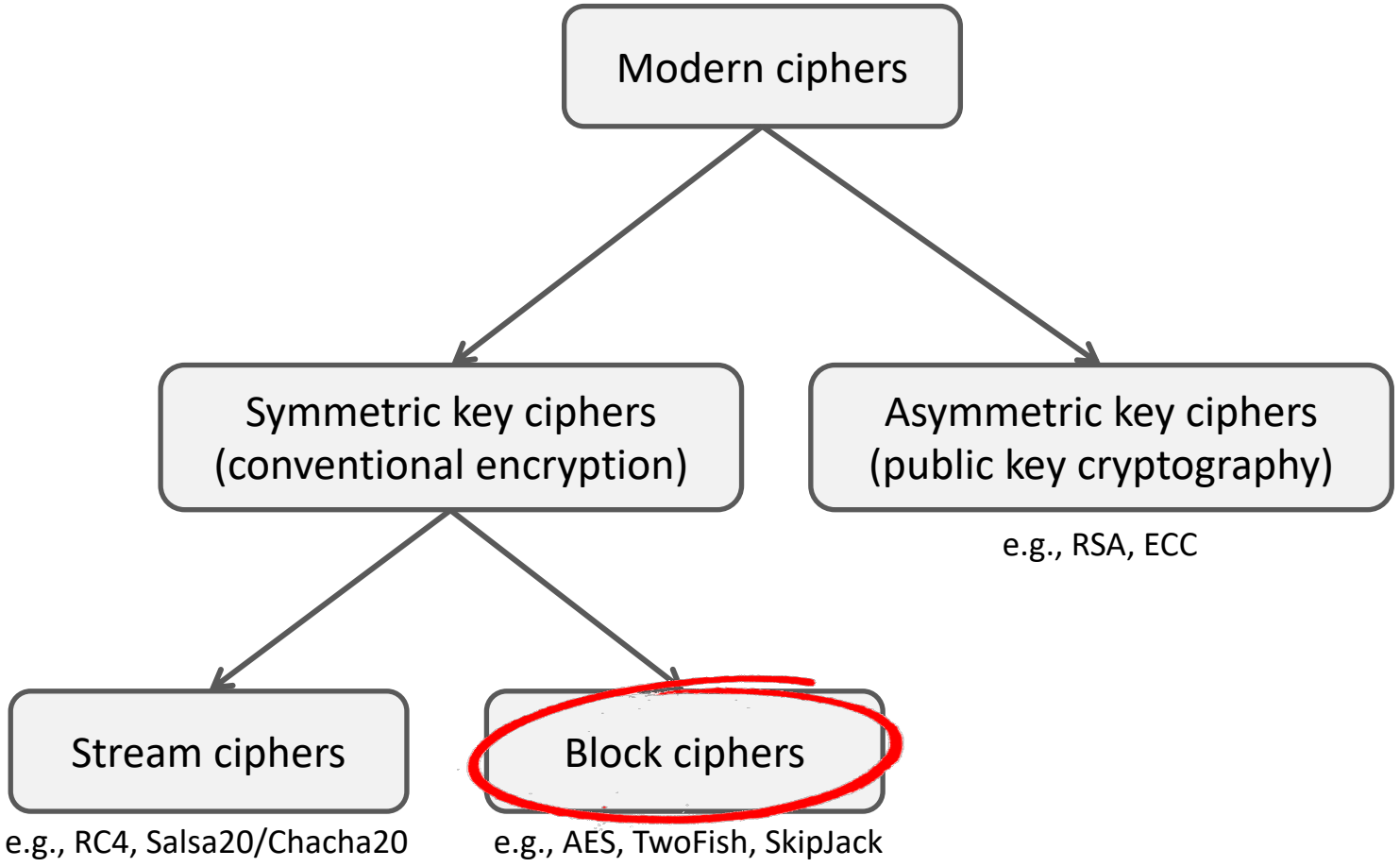
Symmetric Key Encryption
Block Ciphers

Levente Buttyán
CrySyS Lab, BME
buttyan@crysys.hu

Classification of ciphers

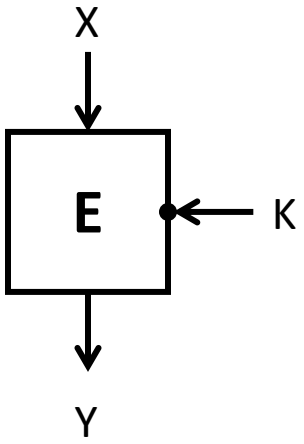


Block ciphers

- block ciphers operate on blocks of bits (typical block size is n = 128 bits)
- they are stateless (unlike stream ciphers)
- they cannot be efficiently distinguished from a random permutation
  - if K is unknown, the output is unpredictable (even parts of it, and even when some input-output pairs are known)

- notation:
  - E(K, X) or $E_K(X)$ for encryption
  - $E_K^{-1}(Y)$ or $D_K(Y)$ for decryption

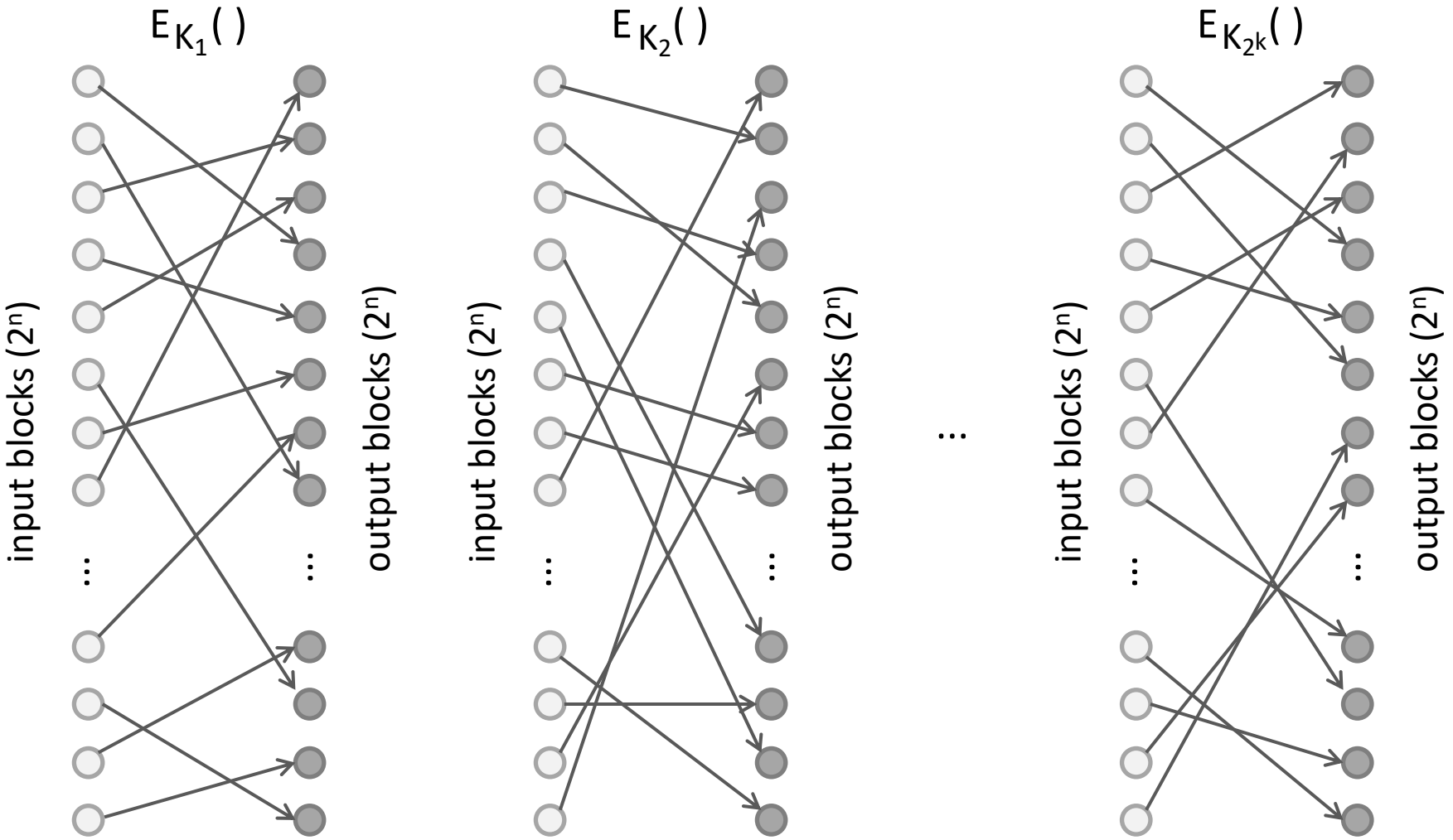
- terminology
  - X – plaintext block (bit vector of length n)
  - Y – ciphertext block (bit vector of length n)
  - K – key (bit vector of length k)
  - E – encryption/encoding algortihm
  - D – decryption/decoding algorithm



Applications of block ciphers

- primarily:
  - encryption of data (of any size, not just one block) → confidentiality
- can also be used as a building block for
  - MAC functions → message integrity and authentication services
  - hash functions
  - PRNGs (Pseudo-Random Number Generators)
  - key-stream generators for stream ciphers

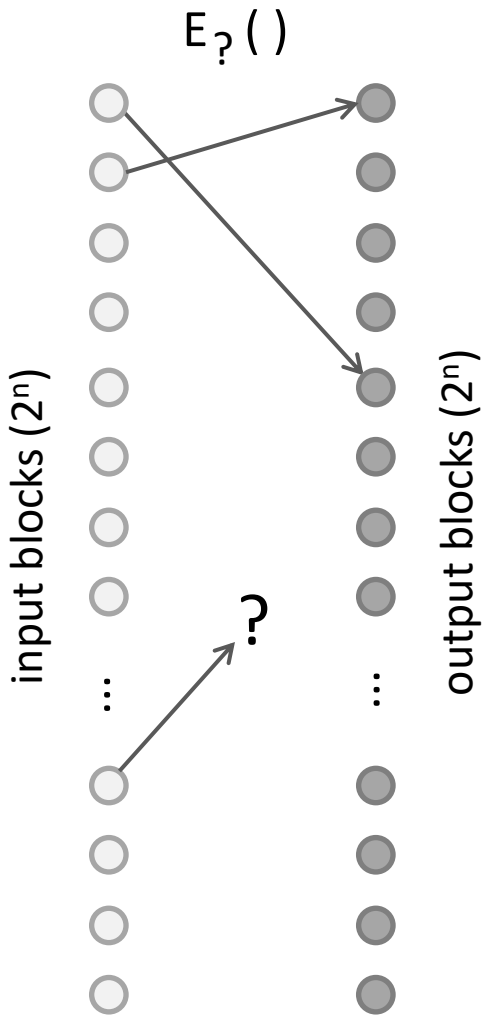
Viewing block ciphers as permutations



~ familiy of permutations indexed by the key

The random permutation model

even if we know where some Xs are mapped (i.e., observed some (X, Y) pairs)...



we cannot predict where a new X will be mapped (all Ys not yet used are equally probable)

Product ciphers

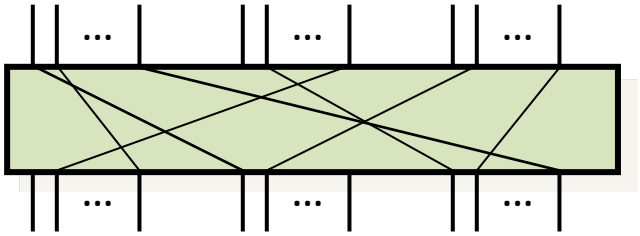
- use multiple layers of simple operations, which offer complementary – but individually insufficient – protection
- careful design ensures that the resulting cipher is more secure than its individual components
- simple operations may include:
  - elementary arithmetic and logical operations (e.g., XOR)
  - modular multiplication
  - substitutions
  - bit-permutations
  - ...
- examples:
  - Shannon's substitution-permutation (SP) network
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)

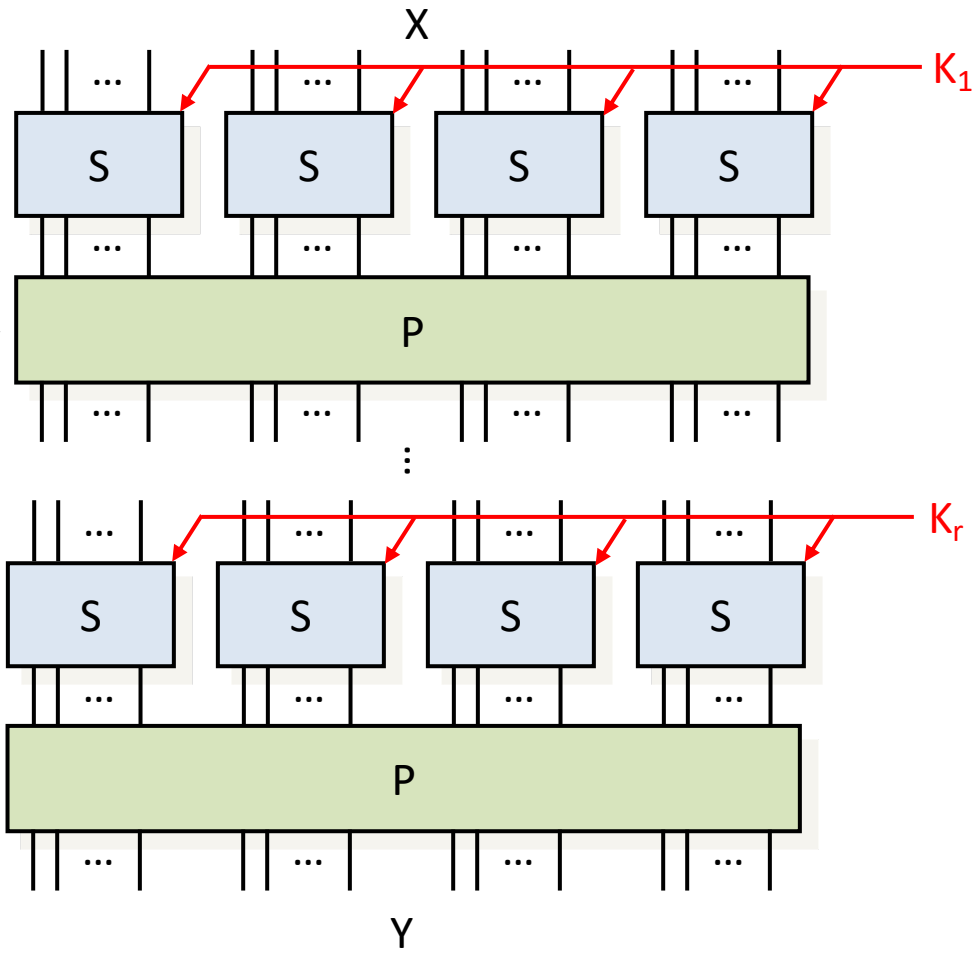
Shannon's SP network

substitution / look-up table:

input	output
0000	0110
0001	0101
0010	1001
0011	1101
...	...
1111	0001

bit-permutation:

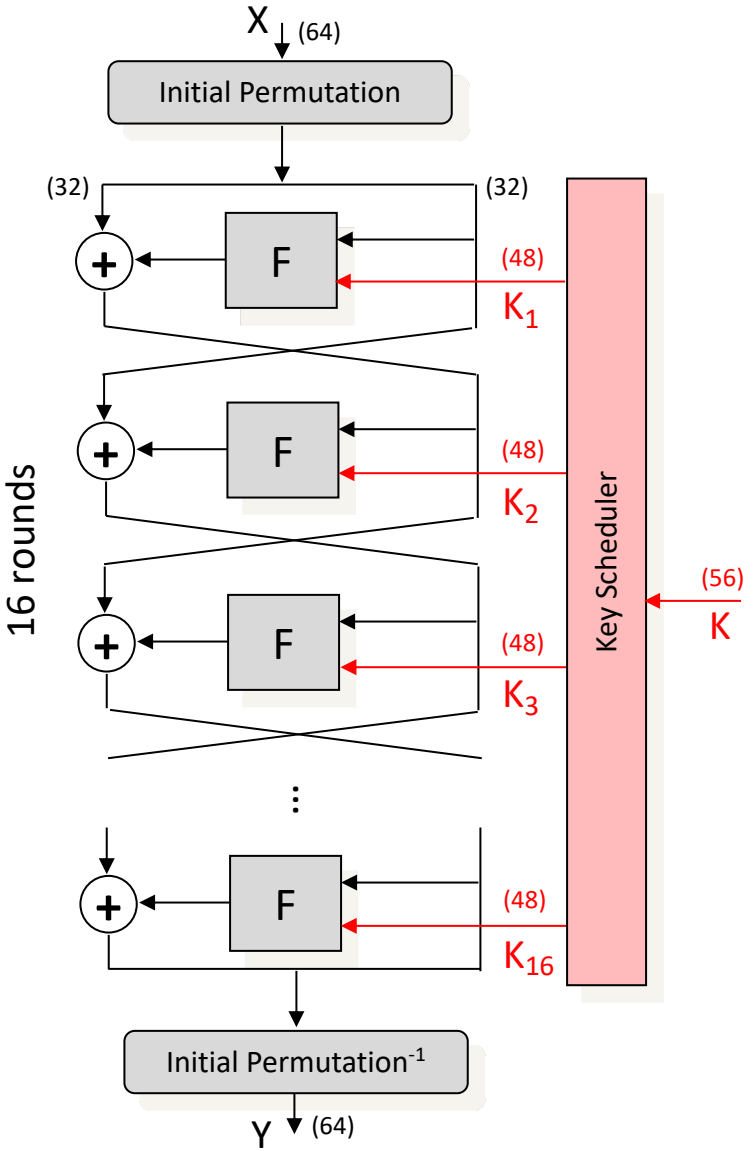




substitutions → "confusion"
permutations → "diffusion"

avalanche effect :
when changing one bit in the input, each output bit changes with probability ~1/2

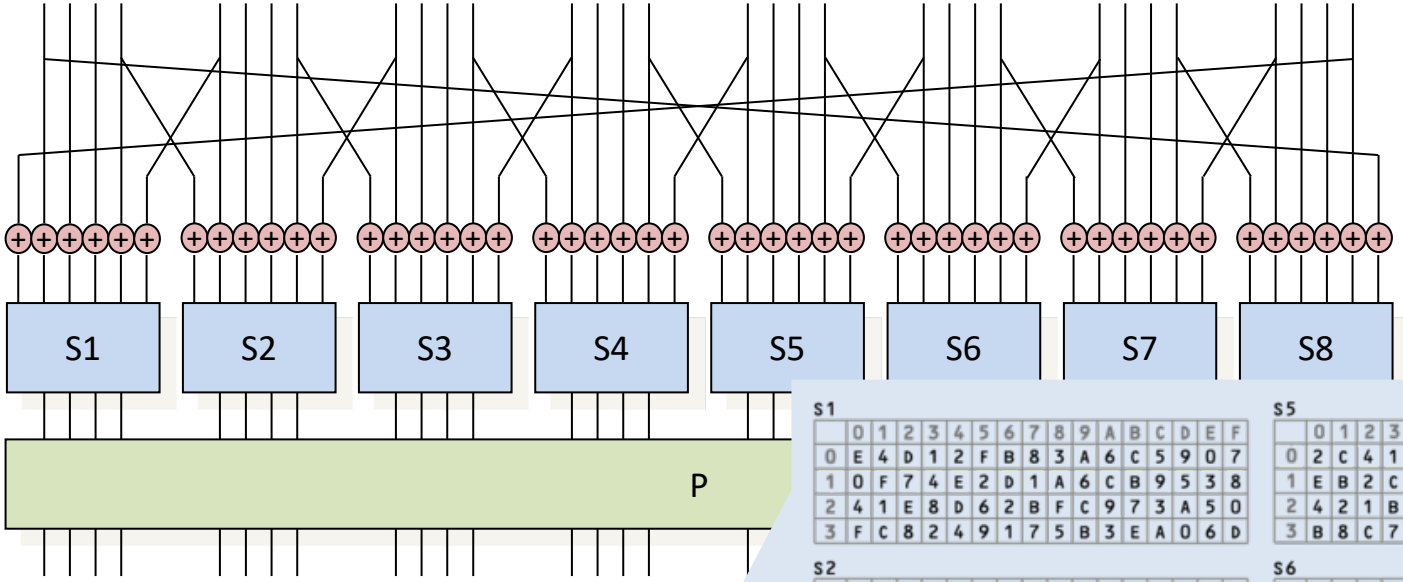
Data Encryption Standard (DES)



- published by NIST in 1977
- replaced by AES in 2001
- in between, adopted and used worldwide

- input size: 64 bits
- output size: 64 bits
- key length: 56 bits
- rounds: 16
- Feistel structure

DES round function F



- Si – substitution box (S-box)
  - » non-linear look-up tables
- P – permutation box (P-box)
  - » linear bit permutation

S1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

S2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
1	3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
2	0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
3	D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9

S3

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
1	D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
2	D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
3	1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C

S4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
1	D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
2	A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3	3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E

S5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
1	E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
2	4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
3	B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3

S6

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
1	A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
2	9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
3	4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D

S7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
1	D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
2	1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
3	6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C

S8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1	1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
2	7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
3	2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

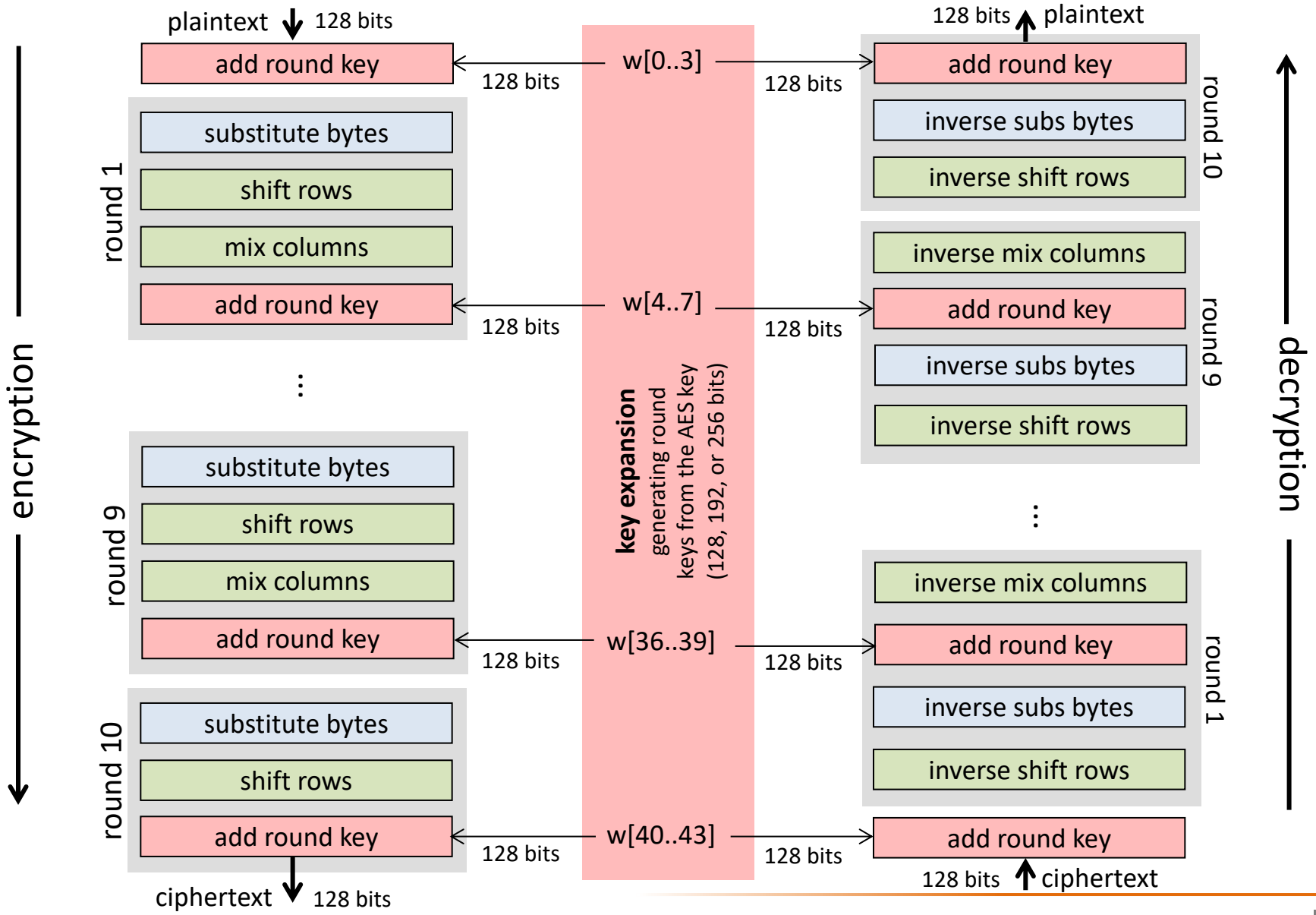
Advanced Encryption Standard (AES)

- NIST asked for proposals to replace DES in the mid 90's
- Rijndael (designed by Vincent Rijmen and Joan Daemen) was selected as the winning proposal in a competitive selection process
- it was then standardized under the name AES in November 2001

- AES parameters:
  - input/output size: 128 128 128
  - key size: 128 192 256

- some other features:
  - multiple rounds (10, 12, or 14, depending on the key size)
  - key injection (bitwise XOR)
  - single S-box (8 bit to 8 bit)
  - no bit permutation → other ways of "mixing" in each round
  - no Feistel structure → decryption algorithm is different from encryption algorithm
    - » decryption uses the inverse of the "mixing" and the S-box
    - » decryption is slower than encryption

AES structure

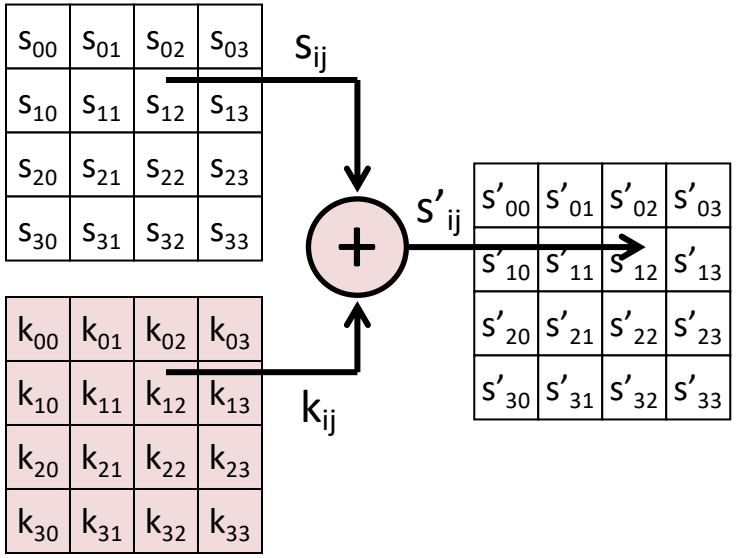


AES internals

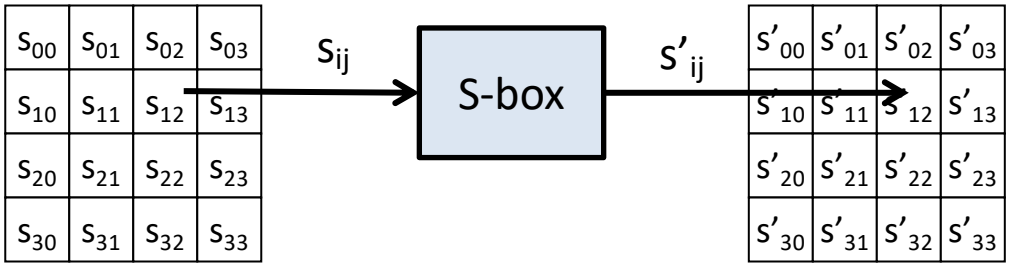
data being processed is represented as a 4x4 matrix:

b_0	b_4	b_8	b_{12}
b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}

add round key

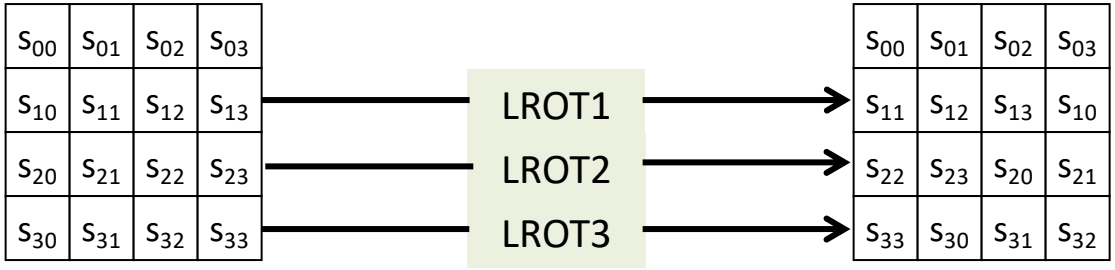


substitute bytes

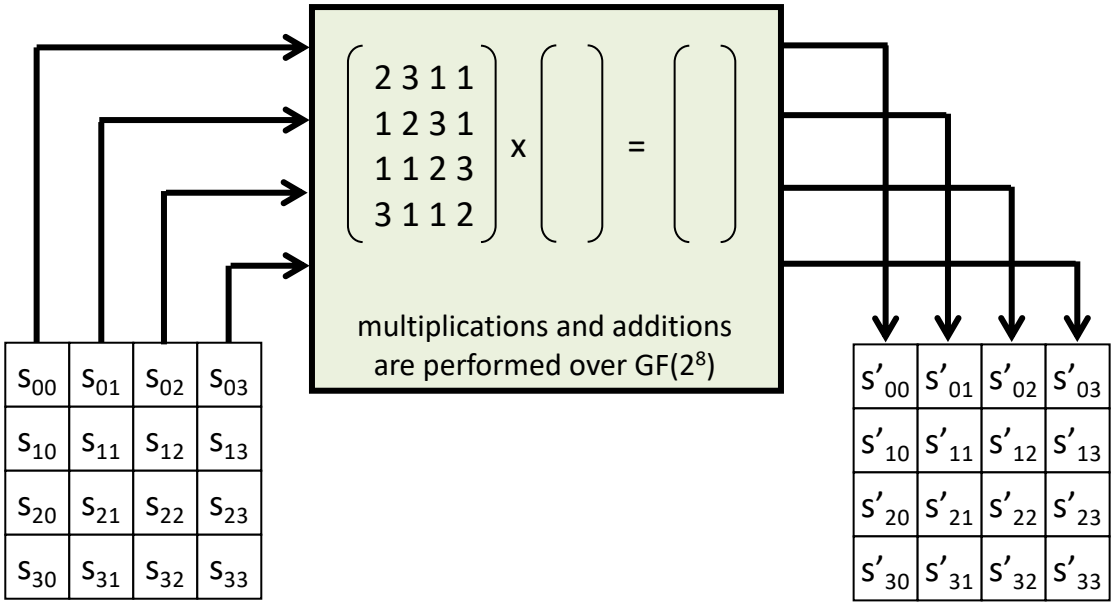


AES internals

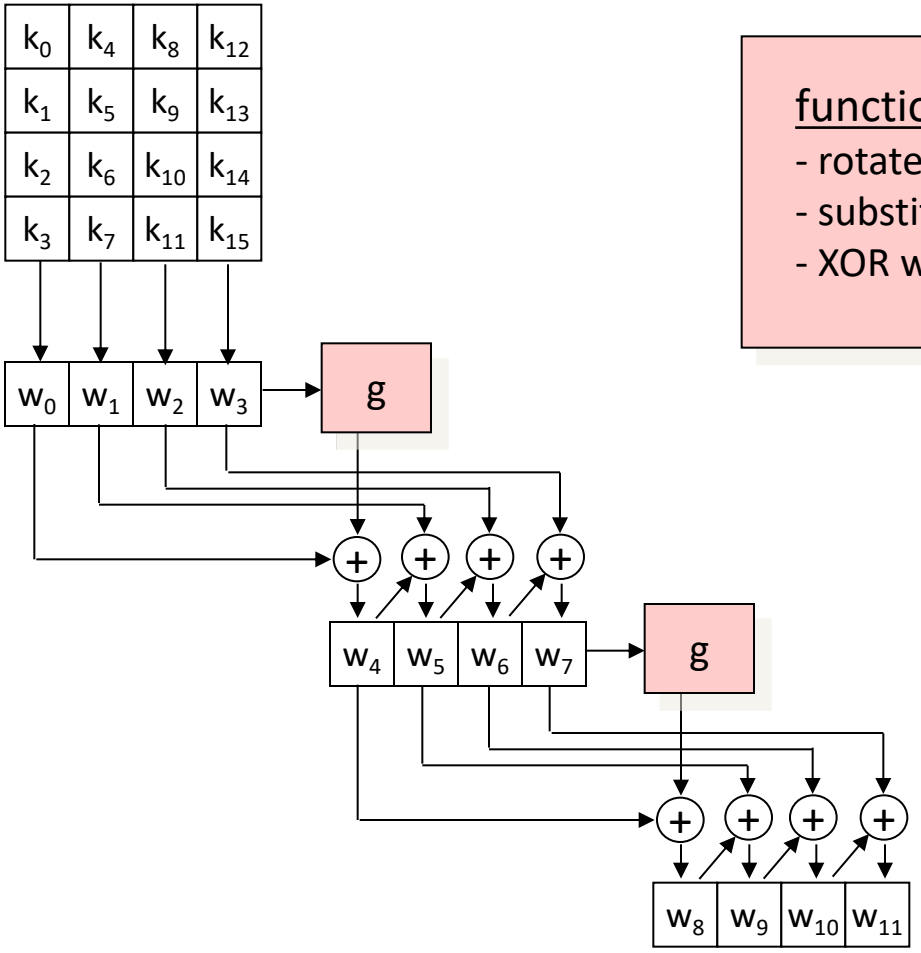
shift row



mix column



AES key expansion



function g
- rotate word
- substitute bytes
- XOR with round constant

Kerckhoffs' principles

JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général LEWAL, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains [1].

Depuis la modeste scytale des Lacédémoniens et les *trucs* inventés ou rapportés par Æneas-le-Tacticien [2], jusqu'au fameux

Auguste Kerckhoffs, « La cryptographie militaire, » Journal des sciences militaires, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Février 1883.

II.

DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE.

Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Tout le monde est d'accord pour admettre la raison d'être des

Openness of specification

- Kerckhoffs' 2nd Principle says that it must be assumed that the encryption algorithm is known to the attacker
  - in other words, the security of the system cannot depend on the secrecy of the algorithm (no security by obscurity)

- advantages of adherence to the 2nd Principle:
  - secrecy of an algorithm can be broken by reverse engineering the implementation or by leaking out design documents (many examples)
  - published designs undergo public scrutiny
  - it is better if security flaws are revealed by "white hat guys"
  - public designs allow for standards

- the other principles are also interesting (note the date: 1883)

Attack models

- attack objectives:
  - systematic decoding of plaintexts
  - figuring out the key (breaking the key)

- attacker capabilities:
  - ciphertext-only attack (basic model)
  - known-plaintext attack (example?)
  - (adaptive) chosen-plaintext attack (example?)
  - (adaptive) chosen-ciphertext attack (example?)

- attack complexity measures:
  - data complexity
  - storage complexity
  - processing complexity
    - » expected number of “basic operations” required for the attack
    - » parallelization may reduce attack time but not processing complexity!

Exhaustive key search (brute force)

- given a small number of plaintext-ciphertext pairs encrypted under a key K, K can be recovered by exhaustive search with 2^{k-1} processing complexity (expected number of en/decryption operations)
  - input: (X, Y), (X', Y'), …
  - progress through the entire key space:
    - » for each candidate key K', decrypt Y
    - » if the result is not X, then throw away K'
    - » if the result is X, then check the other pairs (X', Y'), …
    - » if K' does not work for at least one pair, then throw away K'
  - if K' worked for all pairs (X, Y), (X', Y'), …, then output K' as the target key
  - on average, the target key is found after searching half of the key space

→ **2^{k-1} must be sufficiently large (e.g., k = 128)**

Algebraic attacks

- weaknesses in the algebraic structure of a block cipher may lead to attacks that are *substantially* more efficient than the exhaustive key search attack

- illustrative example: the complementation property of DES can be used to reduce the average complexity of exhaustive key search from 2^{55} to 2^{54}

  complementation property of DES: $Y = DES_K(X)$ implies $Y^* = DES_{K^*}(X^*)$

  where X^* denotes the bitwise complement of X

- real examples: linear and differential cryptanalysis
  - most powerful algebraic attacks against DES-like ciphers
  - linear cryptanalysis (LC) against DES
    - » requires "only" ~2^{43} known plaintext-ciphertext pairs
  - differential cryptanalysis (DC) against DES
    - » requires "only" ~2^{47} chosen plaintext-ciphertext pairs

Double encryption

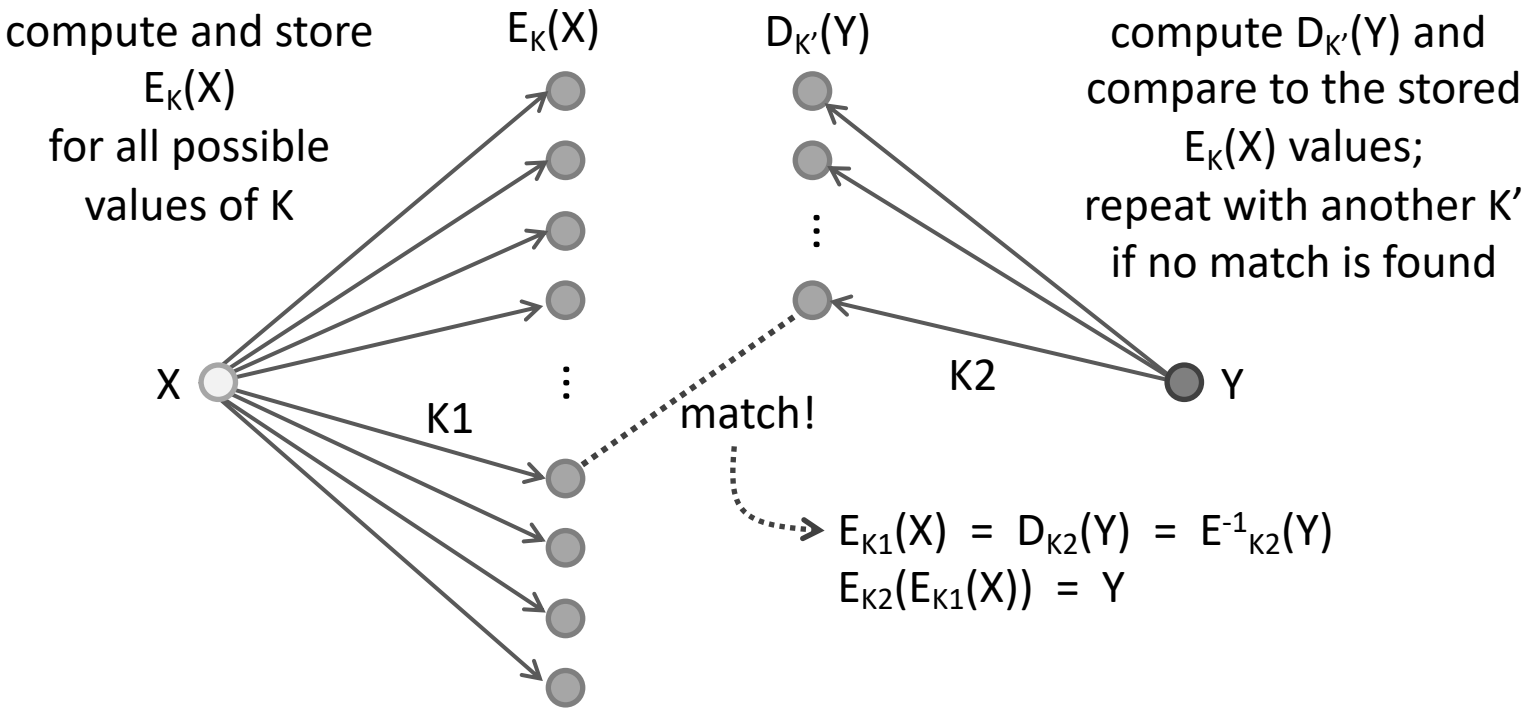
- assume you must use an old block cipher E which has a small key size k (e.g., DES)
- your idea is to double the key size by using E twice on the input with two different keys:

$$Y = E_{K2}(E_{K1}(X))$$

- Are you better off? Did you really significantly increase the complexity of brute force exhaustive key search?

The meet-in-the-middle attack

- let's assume that we have a plaintext-ciphertext pair (X, Y)
- we want to determine (K1, K2) that produced Y from X



storage complexity: ~2^k

processing complexity: at most $2 \times 2^k = 2^{k+1} << 2^{2k}$

The idea of 3DES

- small key size was a real problem for DES, and the following scheme was invented to increase it:

$$Y = DES_{K3}(DES^{-1}_{K2}(DES_{K1}(X)))$$

- (K1, K2, K3) is called ”key bundle”
- keying options:
  - all three keys are independent → key length is 3x56 = 168 bits
  - K1 and K2 are independent, K3 = K1 → key length is 112 bits
    - » stronger then simple double encryption, because it is not subject to the meet-in-the-middle attack
  - K1 = K2 = K3 → equivalent to DES, provides backward compatibility

Block cipher selection criteria

- there are many block ciphers available
  - DES (3DES), AES, RC5, Blowfish, Twofish, Skipjack, ...

- How to choose?
  - design assumptions vs. application requirements
    - » e.g., is it optimized for hardware or software implementations?
  - efficiency
    - » speed
    - » memory size
    - » code size (or number of gates)
  - security
    - » key size (resistence to brute force exhaustive key search)
    - » algebraic properties
    - » complexity of best known attacks
    - » openness of specification (security by obscurity vs. Kerckhoffs' principle)
  - patent issues

Summary on block ciphers

- block ciphers
  - operate on blocks of bits, stateless
  - random permutation model
  - constructions (substitution-permutation networks, DES, AES)
- Kerckhoffs' principle
  - openness vs. ”security by obscurity”
- attacker models
  - attacker objectives and capabilities
- exhasutive key search attack
- double encryption and the meet-in-the-middle attack
- triple encryption and 3DES
- block cipher selection criteria

Control questions

- How block ciphers work? What does it mean intuitively that a block cipher behaves like a random permutation?
- How block ciphers are constructed? What do we mean by an avalanche effect?
- What is the Kerkchoff principle? Why is it important?
- What are the standard attacker models in case of encryption?
- How does exhaustive key search work? What is its complexity?
- For a cipher to be secure, is it sufficient to have a large key size?
- What is double encryption and how does the meet-in-the-middle attack work on it?
- How does 3DES work?
- What are the main block cipher selection criteria?