Block Ciphers

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

December 23, 2022

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

3

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement nor does it imply that the products mentioned are necessarily the best available for the purpose.

Outline

Outline

What is a Block Cipher?

What is a Block Cipher?

Block Cipher

A **block cipher** is a function

$$f_{\mathcal{K}} : \mathcal{P}_A^n \to \mathcal{C}_A^m,$$

such that for each key $K \in \mathcal{K}$, an 'invertible mapping' exists for f_K.

Definition

*A mapping $f_{\{0,1\}^k} : \{0,1\}^n \to \{0,1\}^n$ is called a **block cipher** with block size n bits and key size k bits, if the mapping $f_K(\cdot)$ is a bijection for each $K \in \{0,1\}^k$, i.e., if $f_K^{-1}(\cdot)$ exists with $f_K^{-1}(f_K(x)) = x$ for each $K \in \{0,1\}^k$ & $x \in \{0,1\}^n$.*

Simple Substitution

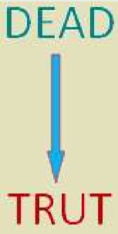
Example

A	B	C	D	E	F	G	H	...	Z
U	I	K	T	R	F	Z	W	...	G

Simple Substitution

Example

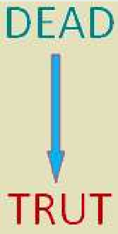
A	B	C	D	E	F	G	H	...	Z
U	I	K	T	R	F	Z	W	...	G

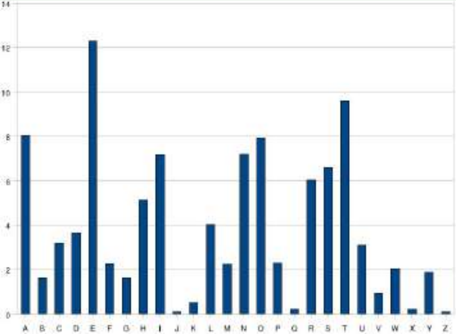


Simple Substitution

Example

A	B	C	D	E	F	G	H	...	Z
U	I	K	T	R	F	Z	W	...	G





Permutation on Block of Characters

Example

AAAA	AAAB	AAAC	$\cdots$	ZZZZ
QAQZ	WIJT	ENTO	$\cdots$	MIHB

Permutation on Block of Characters

Example

AAAA	AAAB	AAAC	$\cdots$	ZZZZ
QAQZ	WIJT	ENTO	$\cdots$	MIHB

- '*code book*'

Permutation on Block of Characters

Example

AAAA	AAAB	AAAC	$\cdots$	ZZZZ
QAQZ	WIJT	ENTO	$\cdots$	MIHB

- '*code book*'
- If blocks are large enough, then frequency analysis becomes impossible (infeasible).

Block Cipher

Block Cipher

- Avoid transport & storage of huge table
- Introduce computation rule to compute table elements:

$$T[X] = f_{key}(X)$$

- Design “good" rule f:

Block Cipher

- Avoid transport & storage of huge table
- Introduce computation rule to compute table elements:

$$T[X] = f_{key}(X)$$

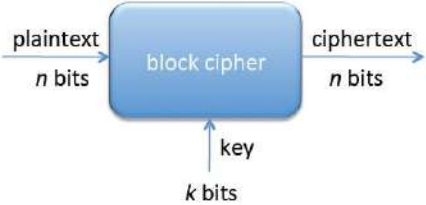
- Design “good" rule f:
  - Secure
  - Efficient

Block Cipher

- A block cipher with n-bit block and k-bit key is a subset of 2^k permutations among all $2^n!$ permutations on n bits.

Block Cipher

- A block cipher with n-bit block and k-bit key is a subset of 2^k permutations among all $2^n!$ permutations on n bits.



Attack Models

An attack model is **a set of assumptions** about how attackers might interact with a cipher and what they can and can't do. The goals of an attack model are as follows:

Attack Models

An attack model is **a set of assumptions** about how attackers might interact with a cipher and what they can and can't do. The goals of an attack model are as follows:

- To set requirements for cryptographers who design ciphers, so that they know what attackers and what kinds of attacks to protect against.

Attack Models

An attack model is **a set of assumptions** about how attackers might interact with a cipher and what they can and can't do. The goals of an attack model are as follows:

- To set requirements for cryptographers who design ciphers, so that they know what attackers and what kinds of attacks to protect against.
- To give guidelines to users, about whether a cipher will be safe to use in their environment.

Attack Models

An attack model is **a set of assumptions** about how attackers might interact with a cipher and what they can and can't do. The goals of an attack model are as follows:

- To set requirements for cryptographers who design ciphers, so that they know what attackers and what kinds of attacks to protect against.
- To give guidelines to users, about whether a cipher will be safe to use in their environment.
- To provide clues for cryptanalysts who attempt to break ciphers, so they know whether a given attack is valid. An attack is only valid if it's doable in the model considered.

Attack Models

An attack model is **a set of assumptions** about how attackers might interact with a cipher and what they can and can't do. The goals of an attack model are as follows:

- To set requirements for cryptographers who design ciphers, so that they know what attackers and what kinds of attacks to protect against.
- To give guidelines to users, about whether a cipher will be safe to use in their environment.
- To provide clues for cryptanalysts who attempt to break ciphers, so they know whether a given attack is valid. An attack is only valid if it's doable in the model considered.

All models are wrong; the practical question is how wrong do they have to be to not be useful – George E. P. Box

Attack Models

Black-Box Model:

Attack Models

Black-Box Model:

- **Ciphertext-only Attack (COA):** the adversary knows nothing but a number of ciphertexts polynomial in the input size.
- **Known Plaintext Attack (KPA):** the adversary has access to a polynomial number of plaintext ciphertext pairs.
- **Chosen Ciphertext Attack (CCA/CCA1 :** the adversary may select a polynomial number of ciphertexts for which to see the plaintext.
- **Chosen Plaintext Attack (CPA/CPA1):** Some attacks only succeed when the plaintexts have a specific form. In order to mount such attacks, Eve must find a way to influence the encrypted plaintexts.
- **Adaptive Chosen Plaintext Attack (ACPA/CPA2):** the adversary submits plaintexts based on previously obtained ciphertexts.
- **Adaptive Chosen Ciphertext Attack (ACCA/CCA2):** the adversary submits ciphertexts based on previously obtained plaintexts.

Attack Models

Gray-Box Model:

- In this model, the attacker has access to a cipher's implementation.
- This makes gray-box model more realistic than black-box models for applications.
- It is more difficult to define than black-box ones because they depend on physical, analog properties rather than just on an algorithm's input and outputs.
- Side-channel attacks are a family of attacks within gray-box model.

Attack Models

White-Box Model:

- In this model, cryptography is deployed in applications that are executed on open devices.
- Attacker has fully- access to the execution platform.
- Internal details of implementations are completely and alterable at will.
- The challenge that white-box cryptography aims to address is to implement a cryptographic algorithm in software in such a way that cryptographic assets remain secure even when subject to white-box attacks.
- Software implementations that resist such white-box attacks are denoted **white-box implementations.**

Computational vs Information-Theoretic Security

- Information-theoretic security implies that absolutely no information about an encrypted message is leaked, even to an eavesdropper with unlimited computational power.

Computational vs Information-Theoretic Security

- Information-theoretic security implies that absolutely no information about an encrypted message is leaked, even to an eavesdropper with unlimited computational power.
- Computational security incorporates two relaxations:
  - Security is only guaranteed against *efficient adversaries* that run for some feasible amount of time.
  - Adversaries can potentially succeed with some **very small probability**.

Definition

A scheme is (t, ϵ)-secure if any adversary running for time at most t succeeds in breaking the scheme with probability at most ϵ.

Security Goals

Cryptographers define two main security goals:

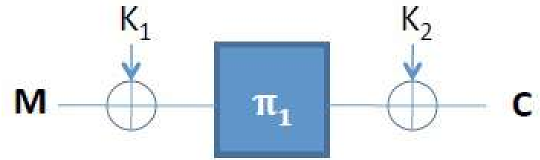
Security Goals

Cryptographers define two main security goals:

- **Indistinguishability (IND)** Ciphertexts should be indistinguishable from random strings.

- **Non-malleability (NM)** Given a ciphertext $C_1 = \mathbb{E}_K(P_1)$, it should be impossible to create another ciphertext, C_2, whose corresponding plaintext, P_2, is related to P_1 in a meaningful way.

Even-Mansour



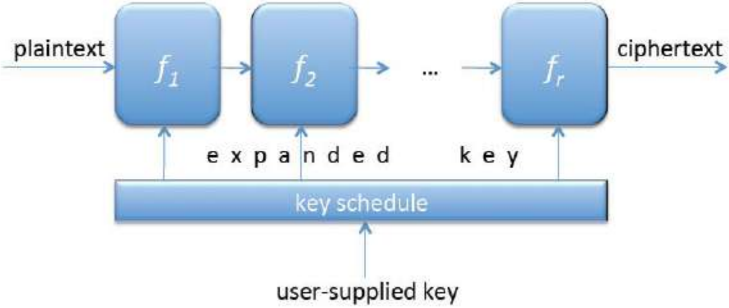
- The Even-Mansour[1] construction is a block cipher.
- Let n be the block-length.
- Fixed public known permutation π_1, where it is easy to compute $\pi(M)$ and $\pi^{-1}(M)$ for any given input $M \in \{0,1\}^n$
- Indistinguishable for $\leq 2^{n/2}$ queries when $\mathbf{A}$ accesses to π_1
- Key recovery attack in $2^{n/2}$ by Daemen Asiacrypt'91

[1] S. Even, Y. Mansour, A Construction of a Cipher From a Single Pseudo-random Permutation, Asiacrypt '91, Springer-Verlag 1992.

Iterative Block Ciphers

- An iterative block cipher consists of r consecutive applications of simpler key-dependent transforms

$$f = f_r \circ f_{r-1} \circ \cdots \circ f_2 \circ f_1$$



Block Cipher Primitives

Block Cipher Primitives

Claude Elwood Shannon

C. E. SHANNON,
Communication Theory of Secrecy Systems, 1949.

Block Cipher Primitives: Confusion and Diffusion

- **Confusion:** is intended to make the relationship between the *key* and *ciphertext* as complex as possible.

Block Cipher Primitives: Confusion and Diffusion

- **Confusion:** is intended to make the relationship between the *key* and *ciphertext* as complex as possible.

  Today, a common element for achieving confusion is substitution/S-box, which is found in both AES and DES.

Block Cipher Primitives: Confusion and Diffusion

- **Confusion:** is intended to make the relationship between the *key* and *ciphertext* as complex as possible.

  Today, a common element for achieving confusion is substitution/S-box, which is found in both AES and DES.

- **Diffusion:** refers to rearranging or spreading out the bits in the message so that any redundancy in the plaintext is spread out over the ciphertext.

Block Cipher Primitives: Confusion and Diffusion

- **Confusion:** is intended to make the relationship between the *key* and *ciphertext* as complex as possible.

  Today, a common element for achieving confusion is substitution/S-box, which is found in both AES and DES.

- **Diffusion:** refers to rearranging or spreading out the bits in the message so that any redundancy in the plaintext is spread out over the ciphertext.

  A simple diffusion element is the bit permutation, which is frequently used within DES.

Block Cipher Primitives: Confusion and Diffusion

- **Confusion:** is intended to make the relationship between the *key* and *ciphertext* as complex as possible.

  Today, a common element for achieving confusion is substitution/S-box, which is found in both AES and DES.

- **Diffusion:** refers to rearranging or spreading out the bits in the message so that any redundancy in the plaintext is spread out over the ciphertext.

  A simple diffusion element is the bit permutation, which is frequently used within DES.

Both operations by themselves cannot provide security. The idea is to concatenate confusion and diffusion elements to build so called product ciphers.

Confusion

Example

Let $\mathbf{x}, \mathbf{y}$ & $\mathbf{k} \in \{0,1\}^8$ and $\mathbf{y} = conf(\mathbf{x}, \mathbf{k})$, where

$$
\begin{aligned}
y_1 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_4 \\
y_2 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \\
y_3 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \\
y_4 &= x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_7 \\
y_5 &= x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_8 \\
y_6 &= x_6 \oplus x_7 \oplus x_8 \oplus x_1 \oplus k_6 \oplus k_7 \oplus k_8 \oplus k_1 \\
y_7 &= x_7 \oplus x_8 \oplus x_1 \oplus x_2 \oplus k_7 \oplus k_8 \oplus k_1 \oplus k_2 \\
y_8 &= x_8 \oplus x_1 \oplus x_2 \oplus x_3 \oplus k_8 \oplus k_1 \oplus k_2 \oplus k_3
\end{aligned}
$$

Confusion

Example

Let $\mathbf{x}, \mathbf{y}$ & $\mathbf{k} \in \{0,1\}^8$ and $\mathbf{y} = conf(\mathbf{x}, \mathbf{k})$, where

$$
\begin{aligned}
y_1 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_4 \\
y_2 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \\
y_3 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \\
y_4 &= x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_7 \\
y_5 &= x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_8 \\
y_6 &= x_6 \oplus x_7 \oplus x_8 \oplus x_1 \oplus k_6 \oplus k_7 \oplus k_8 \oplus k_1 \\
y_7 &= x_7 \oplus x_8 \oplus x_1 \oplus x_2 \oplus k_7 \oplus k_8 \oplus k_1 \oplus k_2 \\
y_8 &= x_8 \oplus x_1 \oplus x_2 \oplus x_3 \oplus k_8 \oplus k_1 \oplus k_2 \oplus k_3
\end{aligned}
$$

It has bad confusion, as they are linear relations.

Diffusion

Example

$$\begin{aligned}
y_1 &= f_1(x_1, x_2, k_1, k_2) \\
y_2 &= f_2(x_2, x_3, k_2, k_3) \\
y_3 &= f_3(x_3, x_4, k_3, k_4) \\
y_4 &= f_4(x_4, x_5, k_4, k_5) \\
y_5 &= f_5(x_5, x_6, k_5, k_6) \\
y_6 &= f_6(x_6, x_7, k_6, k_7) \\
y_7 &= f_7(x_7, x_8, k_7, k_8) \\
y_8 &= f_8(x_8, x_1, k_8, k_1)
\end{aligned}$$

Diffusion

Example

$$
\begin{aligned}
y_1 &= f_1(x_1, x_2, k_1, k_2) \\
y_2 &= f_2(x_2, x_3, k_2, k_3) \\
y_3 &= f_3(x_3, x_4, k_3, k_4) \\
y_4 &= f_4(x_4, x_5, k_4, k_5) \\
y_5 &= f_5(x_5, x_6, k_5, k_6) \\
y_6 &= f_6(x_6, x_7, k_6, k_7) \\
y_7 &= f_7(x_7, x_8, k_7, k_8) \\
y_8 &= f_8(x_8, x_1, k_8, k_1)
\end{aligned}
$$

It has bad diffusion.

Diffusion

Example

$$
\begin{aligned}
y_1 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_4 \\
y_2 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \\
y_3 &= x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus k_3 \oplus k_4 \oplus k_5 \oplus k_6 \\
y_4 &= x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus k_4 \oplus k_5 \oplus k_6 \oplus k_7 \\
y_5 &= x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus k_5 \oplus k_6 \oplus k_7 \oplus k_8 \\
y_6 &= x_6 \oplus x_7 \oplus x_8 \oplus x_1 \oplus k_6 \oplus k_7 \oplus k_8 \oplus k_1 \\
y_7 &= x_7 \oplus x_8 \oplus x_1 \oplus x_2 \oplus k_7 \oplus k_8 \oplus k_1 \oplus k_2 \\
y_8 &= x_8 \oplus x_1 \oplus x_2 \oplus x_3 \oplus k_8 \oplus k_1 \oplus k_2 \oplus k_3
\end{aligned}
$$

Design Criteria

- **Confusion** and **diffusion** methods required to design block ciphers.
- The following methods are applied to design confusion and diffusion

Design Criteria

- **Confusion** and **diffusion** methods required to design block ciphers.
- The following methods are applied to design confusion and diffusion
  1. S-box + Permutation

Design Criteria

- **Confusion** and **diffusion** methods required to design block ciphers.
- The following methods are applied to design confusion and diffusion
  1. S-box + Permutation
  2. S-box + MDS matrix

Design Criteria

- **Confusion** and **diffusion** methods required to design block ciphers.
- The following methods are applied to design confusion and diffusion
  1. S-box + Permutation
  2. S-box + MDS matrix
  3. ARX

Design Criteria

- **Confusion** and **diffusion** methods required to design block ciphers.
- The following methods are applied to design confusion and diffusion
  1. S-box + Permutation
  2. S-box + MDS matrix
  3. ARX (Mod Addition + Rotation & Xoring)

Comparison Among Feistel Networks, SPN and ARX

	Confusion	Diffusion
Feistel	Non-linear function F	Branch swapping
SPN	S-box	Linear transformation
ARX	Modular addition	XOR, Bit rotation

Padding

- Padding for block ciphers is specified in the PKCS#7 and in RFC5652

Padding

- Padding for block ciphers is specified in the PKCS#7 and in RFC5652
- The rules for padding 16-byte blocks
  - If there are one byte left, pad the message with 15 bytes 0f.

Padding

- Padding for block ciphers is specified in the PKCS#7 and in RFC5652
- The rules for padding 16-byte blocks
  - If there are one byte left, pad the message with 15 bytes 0f.
  - If there are two bytes left, pad the message with 14 bytes 0e.

Padding

- Padding for block ciphers is specified in the PKCS#7 and in RFC5652
- The rules for padding 16-byte blocks
  - If there are one byte left, pad the message with 15 bytes 0f.
  - If there are two bytes left, pad the message with 14 bytes 0e.
  - If there are 15 bytes left, pad the message with 1 bytes 01.

Padding

- Padding for block ciphers is specified in the PKCS#7 and in RFC5652
- The rules for padding 16-byte blocks
  - If there are one byte left, pad the message with 15 bytes 0f.
  - If there are two bytes left, pad the message with 14 bytes 0e.
  - If there are 15 bytes left, pad the message with 1 bytes 01.
  - If it is a multiple of 16 bytes, add 16 bytes 10.

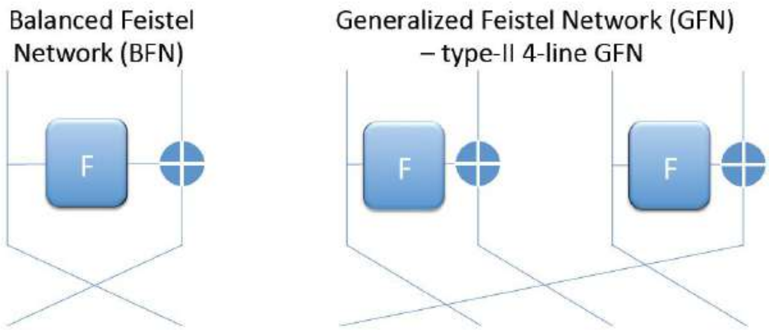
Padding

															01
														02	02
													03	03	03
												04	04	04	04
											05	05	05	05	05
										06	06	06	06	06	06
									07	07	07	07	07	07	07
								08	08	08	08	08	08	08	08
							09	09	09	09	09	09	09	09	09
						0A	0A	0A	0A	0A	0A	0A	0A	0A	0A
					0B	0B	0B	0B	0B	0B	0B	0B	0B	0B	0B
				0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C
			0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
		0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E	0E
	0F	0F	0F	0F	0F	0F	0F	0F	0F	0F	0F	0F	0F	0F	0F
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10

Horst Feistel

Outline

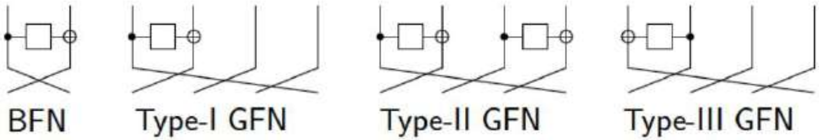
Balanced and Generalized Feistels



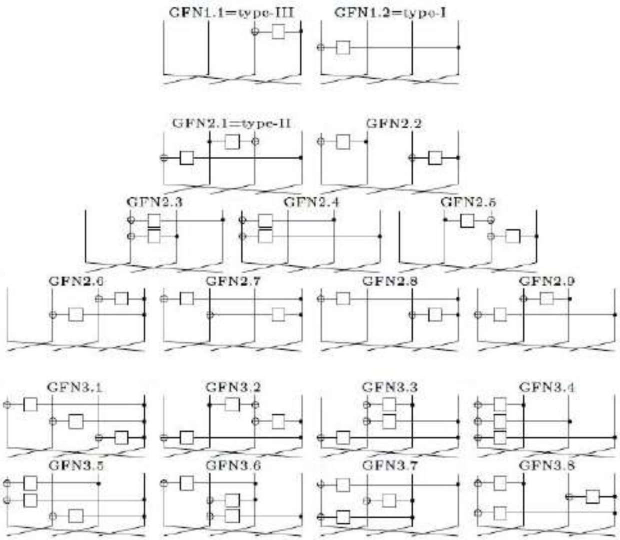
Used in DES, Camellia, E2, Blowfish, Twofish, CAST128, KASUMI, MISTY, ...

Used in CLEFIA, SHAvite-3, RC6,...

Balanced and Generalized Feistels



Classification of 4-line GFNs



Introduction

May 1973	:	NBS issued a call for proposals for a block cipher suitable for federal use
Aug 1974	:	a second call was made
	:	DEA (modified Lucifer) was submitted by IBM.
Mar 1975	:	the algorithm was published for public comment
Aug 1976	:	accepted as a standard
Jan 1977	:	published as FIPS 46

Introduction

May 1973	:	NBS issued a call for proposals for a block cipher suitable for federal use
Aug 1974	:	a second call was made
	:	DEA (modified Lucifer) was submitted by IBM.
Mar 1975	:	the algorithm was published for public comment
Aug 1976	:	accepted as a standard
Jan 1977	:	published as FIPS 46

It was designed by IBM, verified by NSA and published by the NBS.

Introduction

May 1973	:	NBS issued a call for proposals for a block cipher suitable for federal use
Aug 1974	:	a second call was made
	:	DEA (modified Lucifer) was submitted by IBM.
Mar 1975	:	the algorithm was published for public comment
Aug 1976	:	accepted as a standard
Jan 1977	:	published as FIPS 46

It was designed by IBM, verified by NSA and published by the NBS.

2004	:	NIST withdrew DES
2009	:	NIST withdrew 2-key TDES
until 2030	:	3-key TDES

Introduction

DES Development was controversial

Introduction

DES Development was controversial

- NSA secretly involved
- design process was secret
- key length reduced from 128-bit to 56-bit
- two 4×4 S-boxes to eight 6×4 S-boxes
- subtle changes to Lucifer algorithm

DES Numerology

DES is a Feistel cipher with

- 64-bit block length
- 56-bit key length
- 16 rounds
- 48-bit of key used in each round

Encryption Algorithm

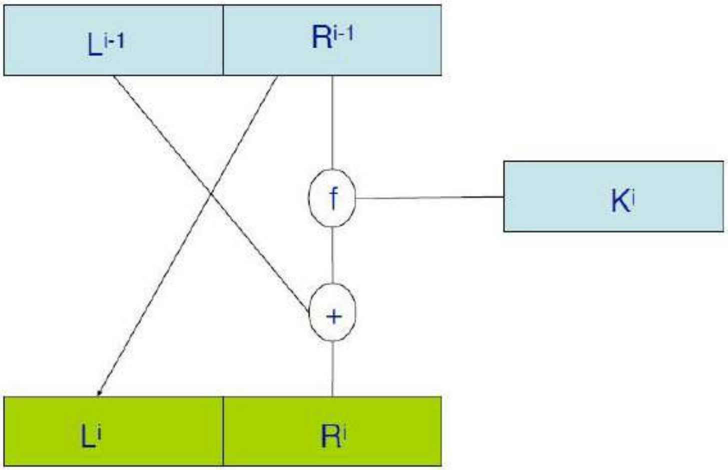
Initial Permutation IP and Inverse Permutation IP^{-1}

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

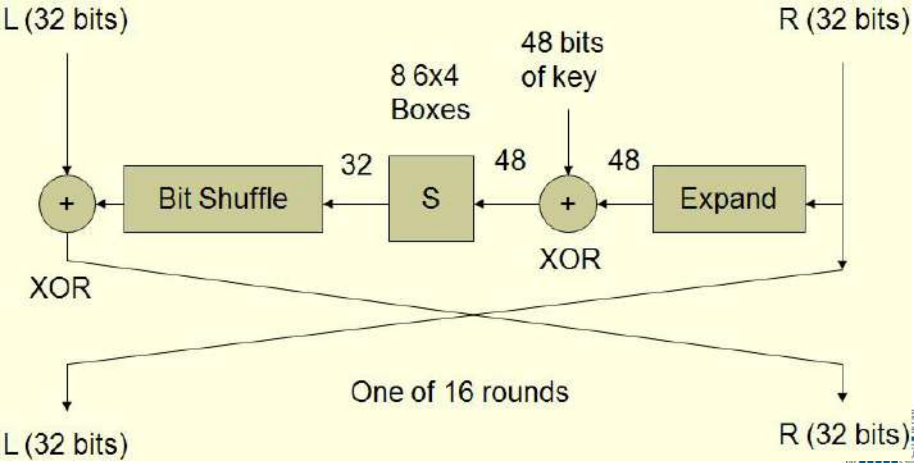
Encryption Algorithm

DES Round Function



Encryption Algorithm

DES Round Function



Encryption Algorithm

Expansion E and Permutation P

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Encryption Algorithm

DES S-boxes

S1	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
p_0	e	4	d	1	2	f	b	8	3	a	6	c	5	9	0	7
p_1	0	f	7	4	e	2	d	1	a	6	c	b	9	5	3	8
p_2	4	1	e	8	d	6	2	b	f	c	9	7	3	a	5	0
p_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
p_0	f	1	8	e	6	b	3	4	9	7	2	d	c	0	5	a
p_1	3	d	4	7	f	2	8	e	c	0	1	a	6	9	b	5
p_2	0	e	7	b	a	4	d	1	5	8	c	6	9	3	2	f
p_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
p_0	a	0	9	e	6	3	f	5	1	d	c	7	b	4	2	8
p_1	d	7	0	9	3	4	6	a	2	8	5	e	c	b	f	1
p_2	d	6	4	9	8	f	3	0	b	1	2	c	5	a	e	7
p_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
p_0	7	d	e	3	0	6	9	a	1	2	8	5	b	c	4	f
p_1	d	8	b	5	6	f	0	3	4	7	2	c	1	a	e	9
p_2	a	6	9	0	c	b	7	d	f	1	3	e	5	2	8	4
p_3	3	f	0	6	a	1	d	8	9	4	5	b	c	7	2	e

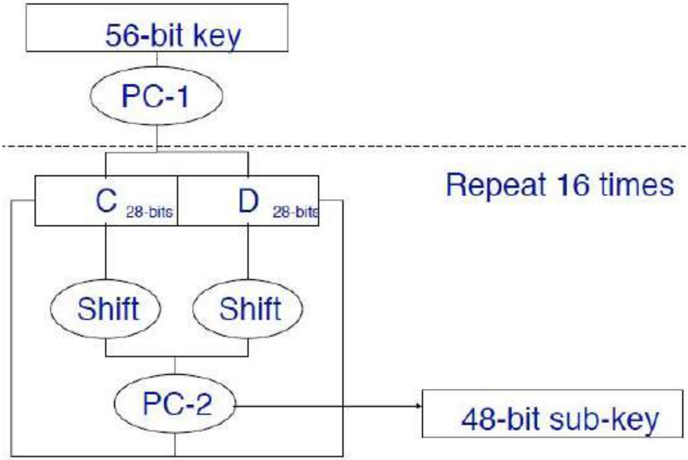
S5	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
p_0	2	c	4	1	7	a	b	6	8	5	3	f	d	0	e	9
p_1	e	b	2	c	4	7	d	1	5	0	f	a	3	9	8	6
p_2	4	2	1	b	a	d	7	8	f	9	c	5	6	3	0	e
p_3	b	8	c	7	1	e	2	d	6	f	0	9	a	4	5	3

S6	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
p_0	c	1	a	f	9	2	6	8	0	d	3	4	e	7	5	b
p_1	a	f	4	2	7	c	9	5	6	1	d	e	0	b	3	8
p_2	9	e	f	5	2	8	c	3	7	0	4	a	1	d	b	6
p_3	4	3	2	c	9	5	f	a	b	e	1	7	6	0	8	d

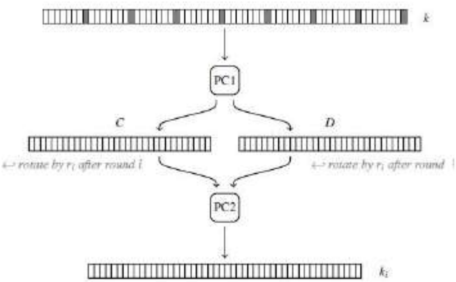
S7	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
p_0	4	b	2	e	f	0	8	d	3	c	9	7	5	a	6	1
p_1	d	0	b	7	4	9	1	a	e	3	5	c	2	f	8	6
p_2	1	4	b	d	c	3	7	e	a	f	6	8	0	5	9	2
p_3	6	b	d	8	1	4	a	7	9	5	0	f	e	2	3	c

S8	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
p_0	d	2	8	4	6	f	b	1	a	9	3	e	5	0	c	7
p_1	1	f	d	8	a	3	7	4	c	5	6	b	0	e	9	2
p_2	7	b	4	1	9	c	e	2	0	6	a	d	f	3	5	8
p_3	2	1	e	7	4	a	8	d	f	c	9	0	3	5	6	b

DES Key Schedule



DES Key Schedule



PC1							PC2					
57	49	41	33	25	17	9	14	17	11	24	1	5
1	58	50	42	34	26	18	3	28	15	6	21	10
10	2	59	51	43	35	27	23	19	12	4	26	8
19	11	3	60	52	44	36	16	7	27	20	13	2
63	55	47	39	31	23	15	41	52	31	37	47	55
7	62	54	46	38	30	22	30	40	51	45	33	48
14	6	61	53	45	37	29	44	49	39	56	34	53
21	13	5	28	20	12	4	46	42	50	36	29	32

round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
r_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES Diffusion

```
Input:     ...............................................................*   1
Permuted:  .......................................*........................   1
Round 1:   .......*........................................................   1
Round 2:   .*..*...*.....*........................*........................   5
Round 3:   .*..*.*.**..*.*.*.*....**.....**.*..*...*.....*................   18
Round 4:   ..*.*****.*.*****.*.*......*.....*..*.*.**..*.*.*.*....**.....**   28
Round 5:   *...**..*.*...*.*.*.*...*.***..*..*.*****.*.*****.*.*......*....   29
Round 6:   ...*..**.....*.*..**.*.**...*..**...**..*.*....*.*.*.*...*.***..*   26
Round 7:   *****...***....**...*..*.*..*......*..**.....*.*..**.*.**...*..*
Round 8:   *.*.*.*.**.....*.*.*...**.*...*******...***....**...*..*.*..*...
Round 9:   ***.*.***...**.*.****.....**.*..*.*.*.*.**.....*.*.*...**.*...**
Round 10:  *.*..*.*.**.*..*.**.***.**.*...****.*.***...**.*.****.....**.*..
Round 11:  ..******......*..******....*....*.*..*.*.**.*..*.**.***.**.*...*
Round 12:  *..***....*...*.*.*.***...****....******......*..******....*....
Round 13:  **..*....*..******...*.........*.*..***....*....*.*.*.***...****..
Round 14:  *.**.*....*.*....**.*...*..**.****..*.....*..******...*.........*.
Round 15:  **.*....*.*.*...*.**.*..*.*.**.**.**.*....*.*....**.*...*..**.**
Round 16:  .*..*.*..*..*.**....**..*..*..****.*....*.*.*...*.**.*..*.*.**.*
Output:    ..*..**.*.*...*....***..***.**.*....*..*..*.*.*.**.*....*.*.*.**.
```

Design Criteria of The S-boxes

- No S-box is a linear or affine function of the input.
- Changing 1 bit in the input to an S-box results in changing at least 2 output bits.
- The S-boxes were chosen to minimize the difference between the number of 1's and 0's when any single bit is held constant.
- For any S-box S, it holds that $S[x]$ and $S[x \oplus 001100]$ differ in at least 2 bits.
- For any S-box S, it holds that $S[x] \neq S[x \oplus 11rs00]$ for any binary values r and s.
- If 2 different 48-bit inputs to the 8 S-boxes result in equal outputs, then there must be different inputs to at least 3 neighbouring S-boxes.
- For any S-box it holds for any non-zero 6-bit value α and for any 4-bit value β, that the number of solutions for x to the equation $S[x] \oplus S[x \oplus \alpha] = \beta$ is at most 16.

Properties of The P Permutation

- The 4 bits output from an S-box are distributed so that they affect 6 different S-boxes in the following round (4 boxes directly and 2 via the expansion mapping).
- If an output bit from S-box i affects one of the 2 middle input bits to S-box j (in the next round), then an output bit from S-box i cannot affect a middle bit of S-box i.
- The middle 6 inputs to 2 neighbouring S-boxes (those not shared by any other S-boxes) are constructed from the outputs from 6 different S-boxes in the previous round.
- The middle 10 input bits to 3 neighbouring S-boxes, 4 bits from the 2 outer S-boxes and 6 from the middle S-box (i.e., those not shared by any other S-boxes), are constructed from the outputs from all S-boxes in the previous round.

Structural Properties

Complementation Property

$$\overline{DES_k(m)} = DES_{\bar{k}}(\bar{m}).$$

Structural Properties

Weak Keys

Definition

A DES key k is said to be weak if the following relationship holds

$$DES_k(DES_k(m)) = m, \quad \forall\, m.$$

4 weak keys of DES

0101010101010101	fefefefefefefefe
1f1f1f1f1f1f1f1f	e0e0e0e0e0e0e0e0

Structural Properties

Semi-Weak Keys

Definition

A pair of keys k_1 & k_2 is said to be semi-weak keys if the following relation satisfies

$$DES_{k_1}(DES_{k_2}(m)) = m, \quad \forall\, m.$$

6 pairs of semi-weak keys of DES

01fe01fe01fe01fe	1fe01fe01fe01fe0	01e001e001e001e0
fe01fe01fe01fe01	e01fe01fe01fe01f	e001e001e001e001
1ffe1ffe1ffe1ffe	011f011f011f011f	e0fee0fee0fee0fe
fe1ffe1ffe1ffe1f	1f011f011f011f01	fee0fee0fee0fee0

Weak Permutation

Definition

A permutation F is called a weak permutation if given

$$y_1 = F_k(x_1) \;\; \& \;\; y_2 = F_k(x_2)$$

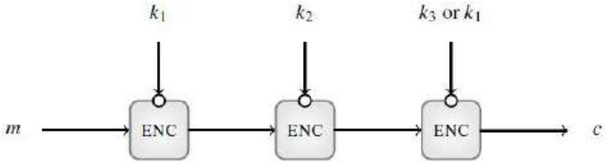
it is 'easy' to extract the key k.

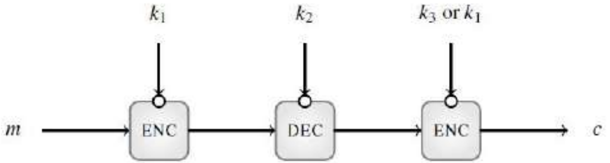
Question

Does 3 rounds of DES form a weak permutation?

Common Proposals for Triple Encryption Using a Generic Block Cipher

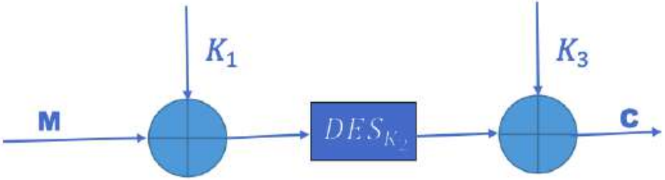
2-key ENC-DEC-ENC	EDE_2	$c = \text{ENC}_{k_1}(\text{DEC}_{k_2}(\text{ENC}_{k_1}(m)))$
2-key ENC-ENC-ENC	EEE_2	$c = \text{ENC}_{k_1}(\text{ENC}_{k_2}(\text{ENC}_{k_1}(m)))$
3-key ENC-DEC-ENC	EDE_3	$c = \text{ENC}_{k_3}(\text{DEC}_{k_2}(\text{ENC}_{k_1}(m)))$
3-key ENC-ENC-ENC	EEE_3	$c = \text{ENC}_{k_3}(\text{ENC}_{k_2}(\text{ENC}_{k_1}(m)))$





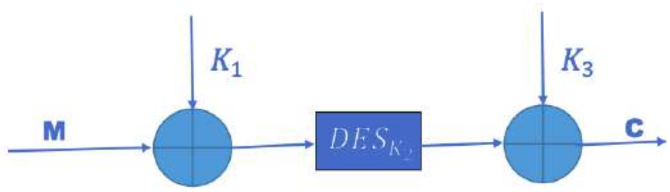
DESX

1. The last algorithm of the DES family is **DESX**
2. This is proposed by Ronald Rivest intended to increase complexity by **applying key whitening**



DESX

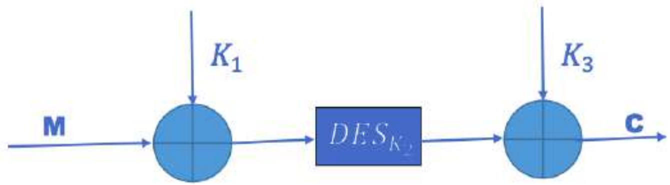
1. The last algorithm of the DES family is **DESX**
2. This is proposed by Ronald Rivest intended to increase complexity by **applying key whitening**



- It requires 184 key bits

DESX

1. The last algorithm of the DES family is **DESX**
2. This is proposed by Ronald Rivest intended to increase complexity by **applying key whitening**



- It requires 184 key bits
- Effective key bits ≈ 118

Outline

Joan Daemen

Vincent Rijmen

Introduction I

Jan 1997	:	NIST announced the initiation.
Sep 1997	:	published the final request for candidate nominations.

The functional requirements

- support block length of 128 bits.
- support key length of 128, 192 and 256 bits.
- as secure as T-DES but much more efficient.
- the encryption scheme available on a world wide royalty-free basis.

Aug 1998	:	15 candidates accepted for the 1^{st} AES candidate conference.
Mar 1999	:	after the 1^{st} evaluation NIST selected 5 finalists.

Introduction II

Rijndael	(86)
Serpent	(59)
RC6	(31)
Mars	(23)
Twofish	(13)

Oct 2000	:	NIST announced that Rijndael was “the best overall algorithm for the AES".
Nov 2001	:	Dept of Commerce officially declared Rijndael as the AES. (FIPS 197)
May 2002	:	AES is effective

Review of AES

NIST Requests Public Comments on Several Existing Cryptography Standards and Special Publications

As part of a periodic review of its cryptography standards and NIST Special Publications, NIST is requesting comments on FIPS 197, SP 800-38A (and Addendum), SP 800-15, SP 800-25, and SP 800-32. Comments are due by June 11, 2021.

May 10, 2021

NIST is in the process of a periodic review and maintenance of its cryptography standards and NIST Special Publications. A description of the review process is available at the Crypto Publication Review Project page.

Currently, we are reviewing the following publications:

- Federal Information Processing Standard (FIPS) 197, *Advanced Encryption Standard (AES)*, 2001
- NIST Special Publication (SP) 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, 2001
- NIST SP 800-38A Addendum, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, 2010

ORGANIZATIONS

Information Technology Laboratory
Computer Security Division
Cryptographic Technology Group

SIGN UP FOR UPDATES FROM NIST

https://www.nist.gov/news-events/news/2021/05/nist-requests-public-comments-several-existing-cryptography-standards-and

Review of AES

NIST Requests Public Comments on Several Existing Cryptography Standards and Special Publications

As part of a periodic review of its cryptography standards and NIST Special Publications, NIST is requesting comments on FIPS 197, SP 800-38A (and Addendum), SP 800-15, SP 800-25, and SP 800-32. Comments are due by June 11, 2021.

May 10, 2021

NIST is in the process of a periodic review and maintenance of its cryptography standards and NIST Special Publications. A description of the review process is available at the Crypto Publication Review Project page.

Currently, we are reviewing the following publications:

- Federal Information Processing Standard (FIPS) 197, *Advanced Encryption Standard (AES)*, 2001
- NIST Special Publication (SP) 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, 2001
- NIST SP 800-38A Addendum, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, 2010

ORGANIZATIONS

Information Technology Laboratory
Computer Security Division
Cryptographic Technology Group

SIGN UP FOR UPDATES FROM NIST

https://www.nist.gov/news-events/news/2021/05/nist-requests-public-comments-several-existing-cryptography-standards-and

https://csrc.nist.gov/projects/crypto-publication-review-project

AES Numerology

AES is a SPN cipher with

- 128-bit block length
- 128-, 192- or 256-bit key length
- 10, 12 or 14 rounds

Mathematical Background

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Mathematical Background

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

Mathematical Background

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

Mathematical Background

- **Addition (in the field $GF(2^8)$)**
  The sum of two elements is the polynomial with coefficients that are given by the sum modulo 2 of the coefficients of the two terms.

Example

$$57 + 83 = ?$$

$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$

$01010111 \oplus 10000011 = 11010100 = D4$

Mathematical Background

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8

$$m(x) = x^8 + x^4 + x^3 + x + 1 or 11B.$$

Mathematical Background

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8

$$m(x) = x^8 + x^4 + x^3 + x + 1 or 11B.$$

Example

$$57 \times 83 = ?$$

Mathematical Background

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8

$$m(x) = x^8 + x^4 + x^3 + x + 1 or 11B.$$

Example

$$57 \times 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$$
$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

Mathematical Background

- **Multiplication**
  Multiplication in $GF(2^8)$ corresponds with multiplication of polynomials modulo an irreducible polynomial over $GF(2)$ of degree 8

$$m(x) = x^8 + x^4 + x^3 + x + 1 or 11B.$$

Example

$$57 \times 83 = ?$$

$$(x^6 + x^4 + x^2 + x + 1) \times (x^7 + x + 1)$$

$$= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

$$(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \; mod \; m(x)$$

$$= x^7 + x^6 + 1 = C1$$

Mathematical Background

Choice of Irreducible Polynomial

- AES uses arithmetic in $GF(2^8)$ with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
- There are 30 irreducible polynomials among which 16 are primitive polynomials.
- It is irrelevant whether the irreducible polynomial is primitive or not, due to the isomorphism of all fields of $GF(2^8)$.
- The isomorphism transformation that takes one description of a cipher under an irreducible polynomial to another description with a different irreducible polynomial is linear.
- There is no advantage to select a primitive polynomial over the current polynomial of Rijndael.

Mathematical Background

- **The extended algorithm of Euclid**
  The multiplication defined above is associative and there is an identity element ('01'). For any polynomial $b(x)$ of degree at most 7 over $GF(2)$, the extended algorithm of Euclid can be used to compute polynomials $a(x)$, $c(x)$ such that

$$b(x)a(x) + m(x)c(x) = 1.$$

  It follows that the set of 256 possible byte values, with the *XOR* as addition and the *multiplication* defined as above has the structure of the finite field $GF(2^8)$.

Mathematical Background

- **Multiplication by x**
  If we multiply $b(x)$ by the polynomial x, we have :

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

- $(x * b(x))$ is obtained by reducing the above result mod $m(x)$.
  i. If $b_7 = 0$, the reduction is identity operation;
  ii. if $b_7 = 1$, $m(x)$ must be subtracted.

Example

$$57 \times 13 = 57 \times (01 \oplus 02 \oplus 10)$$

Mathematical Background

- **Multiplication by x**
  If we multiply $b(x)$ by the polynomial x, we have :

$$b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

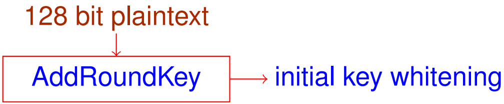
- $(x * b(x))$ is obtained by reducing the above result mod $m(x)$.
  i. If $b_7 = 0$, the reduction is identity operation;
  ii. if $b_7 = 1$, $m(x)$ must be subtracted.

Example

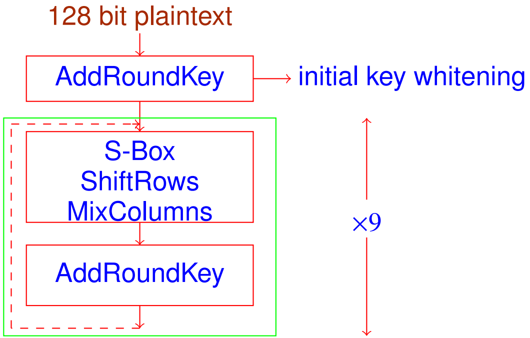
$$57 \times 13 = 57 \times (01 \oplus 02 \oplus 10)$$

$$= 57 \oplus AE \oplus 07 = FE.$$

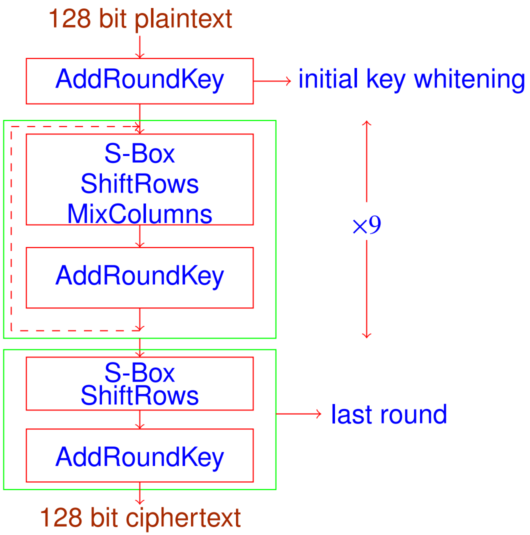
AES-128-Bit Encryption



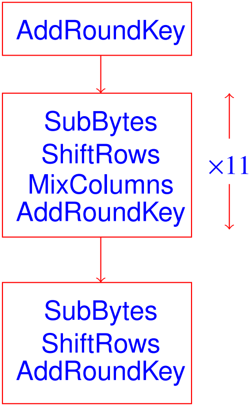
AES-128-Bit Encryption



AES-128-Bit Encryption



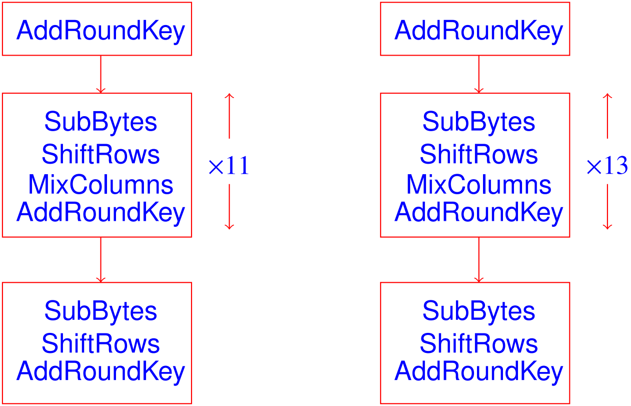
AES-192- & AES-256-Bit Encryption



AES-192

C. Cid, S. Murphy & M. Robshaw,
Algebraic Aspects of the Advanced Encryption Standard, Springer, 2006.

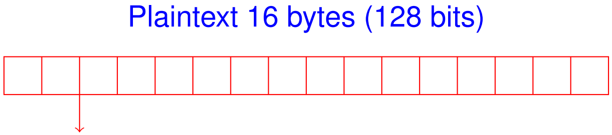
AES-192- & AES-256-Bit Encryption



AES-192 **AES-256**

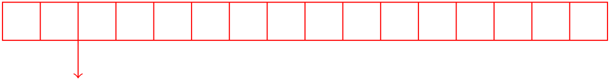
C. Cid, S. Murphy & M. Robshaw,
Algebraic Aspects of the Advanced Encryption Standard, Springer, 2006.

AES-128



AES-128

Plaintext 16 bytes (128 bits)



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}

AES-128

Plaintext 16 bytes (128 bits)

$$\begin{array}{|c|c|c|c|}\hline b_0 & b_4 & b_8 & b_{12} \\ \hline b_1 & b_5 & b_9 & b_{13} \\ \hline b_2 & b_6 & b_{10} & b_{14} \\ \hline b_3 & b_7 & b_{11} & b_{15} \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|}\hline k_0 & k_4 & k_8 & k_{12} \\ \hline k_1 & k_5 & k_9 & k_{13} \\ \hline k_2 & k_6 & k_{10} & k_{14} \\ \hline k_3 & k_7 & k_{11} & k_{15} \\ \hline \end{array}$$

AES-128

Plaintext 16 bytes (128 bits)

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}

$\oplus$

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

↓

$S(b_0 \oplus k_0)$	$S(b_4 \oplus k_4)$	$S(b_8 \oplus k_8)$	$S(b_{12} \oplus k_{12})$
$S(b_1 \oplus k_1)$	$S(b_5 \oplus k_5)$	$S(b_9 \oplus k_9)$	$S(b_{13} \oplus k_{13})$
$S(b_2 \oplus k_2)$	$S(b_6 \oplus k_6)$	$S(b_{10} \oplus k_{10})$	$S(b_{14} \oplus k_{14})$
$S(b_3 \oplus k_3)$	$S(b_7 \oplus k_7)$	$S(b_{11} \oplus k_{11})$	$S(b_{15} \oplus k_{15})$

Design Criteria of AES S-Box

The AES S-Box is the composition of the following 3 functions:

1. $\phi_1 : GF(2^8) \rightarrow GF(2^8)$

$$\begin{array}{ccccccc} f & \mapsto & f^{-1} & \text{if} & f & \neq & 0 \\ & \mapsto & 0 & \text{if} & f & = & 0 \end{array}$$

Design Criteria of AES S-Box

The AES S-Box is the composition of the following 3 functions:

1. $\phi_1 : GF(2^8) \rightarrow GF(2^8)$

$$\begin{array}{lllllll} f & \mapsto & f^{-1} & \text{if} & f & \neq & 0 \\ & \mapsto & 0 & \text{if} & f & = & 0 \end{array}$$

2. $L : GF(2^8) \rightarrow GF(2^8)$

$$f \mapsto (x^4 + x^3 + x^2 + x + 1).f \mod (x^8 + 1)$$

Design Criteria of AES S-Box

The AES S-Box is the composition of the following 3 functions:

1. $\phi_1 : GF(2^8) \to GF(2^8)$

$$\begin{array}{rcllll} f & \mapsto & f^{-1} & \text{if} & f \neq & 0 \\ & \mapsto & 0 & \text{if} & f = & 0 \end{array}$$

2. $L : GF(2^8) \to GF(2^8)$

$$f \mapsto (x^4 + x^3 + x^2 + x + 1).f \mod (x^8 + 1)$$

3. $\phi_2 : GF(2^8) \to GF(2^8)$

$$f \mapsto (x^6 + x^5 + x + 1) + f$$

S-box $= \phi_2 \circ \mathbf{L} \circ \phi_1$.

AES S-box

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES-128

$S(b_0 \oplus k_0)$	$S(b_4 \oplus k_4)$	$S(b_8 \oplus k_8)$	$S(b_{12} \oplus k_{12})$
$S(b_1 \oplus k_1)$	$S(b_5 \oplus k_5)$	$S(b_9 \oplus k_9)$	$S(b_{13} \oplus k_{13})$
$S(b_2 \oplus k_2)$	$S(b_6 \oplus k_6)$	$S(b_{10} \oplus k_{10})$	$S(b_{14} \oplus k_{14})$
$S(b_3 \oplus k_3)$	$S(b_7 \oplus k_7)$	$S(b_{11} \oplus k_{11})$	$S(b_{15} \oplus k_{15})$

AES-128

$S(b_0 \oplus k_0)$	$S(b_4 \oplus k_4)$	$S(b_8 \oplus k_8)$	$S(b_{12} \oplus k_{12})$
$S(b_1 \oplus k_1)$	$S(b_5 \oplus k_5)$	$S(b_9 \oplus k_9)$	$S(b_{13} \oplus k_{13})$
$S(b_2 \oplus k_2)$	$S(b_6 \oplus k_6)$	$S(b_{10} \oplus k_{10})$	$S(b_{14} \oplus k_{14})$
$S(b_3 \oplus k_3)$	$S(b_7 \oplus k_7)$	$S(b_{11} \oplus k_{11})$	$S(b_{15} \oplus k_{15})$

Apply ShiftRows

$S(b_0 \oplus k_0)$	$S(b_4 \oplus k_4)$	$S(b_8 \oplus k_8)$	$S(b_{12} \oplus k_{12})$
$S(b_5 \oplus k_5)$	$S(b_9 \oplus k_9)$	$S(b_{13} \oplus k_{13})$	$S(b_1 \oplus k_1)$
$S(b_{10} \oplus k_{10})$	$S(b_{14} \oplus k_{14})$	$S(b_2 \oplus k_2)$	$S(b_6 \oplus k_6)$
$S(b_{15} \oplus k_{15})$	$S(b_3 \oplus k_3)$	$S(b_7 \oplus k_7)$	$S(b_{11} \oplus k_{11})$

Mix Columns

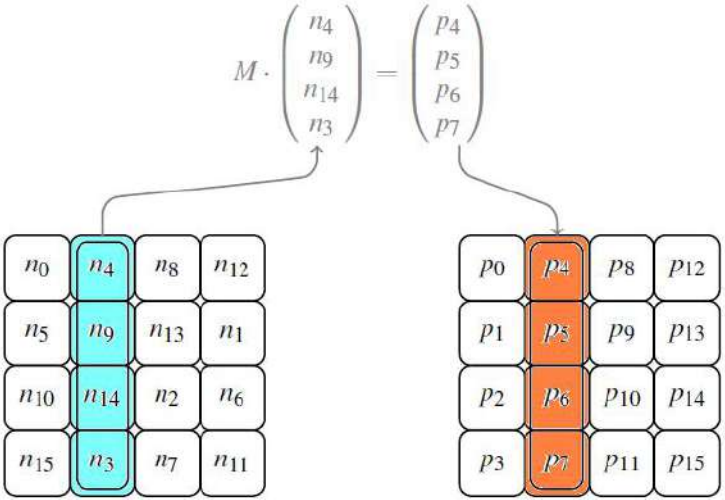
- In mix columns transformation each column is considered as a polynomial over $GF(2^8)$ of degree 3 and multiplied with a fixed polynomial

$$03.x^3 + 01.x^2 + 01.x + 02 \ (mod \ x^4 + 1).$$

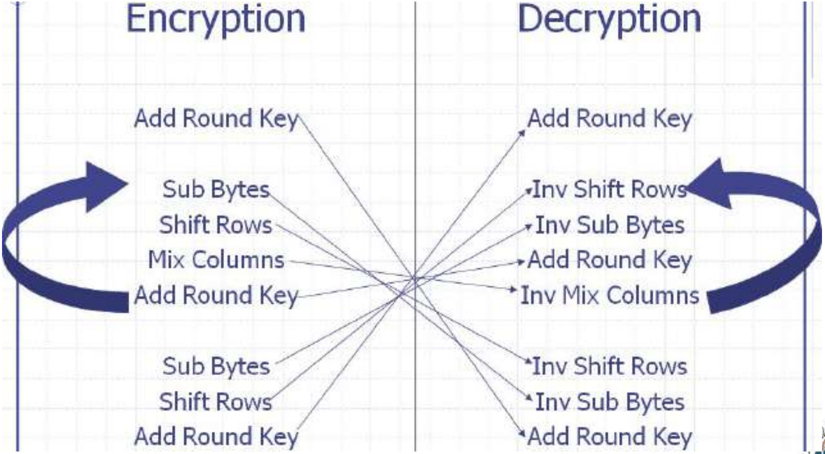
- Mix columns transformation can also be represented by a matrix M multiplication, where

$$M = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

Mix Columns


$M \cdot \begin{pmatrix} n_4 \\ n_9 \\ n_{14} \\ n_3 \end{pmatrix} = \begin{pmatrix} p_4 \\ p_5 \\ p_6 \\ p_7 \end{pmatrix}$
n_0 n_4 n_8 n_{12}
n_5 n_9 n_{13} n_1
n_{10} n_{14} n_2 n_6
n_{15} n_3 n_7 n_{11}
p_0 p_4 p_8 p_{12}
p_1 p_5 p_9 p_{13}
p_2 p_6 p_{10} p_{14}
p_3 p_7 p_{11} p_{15}

Encryption and Decryption



Inverse S-box

$S^{-1}[\cdot]$																
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

AES Key Schedule

1. It takes a 4-word (128 bits) key and produces a linear array of 44 words (1408 bits).
2. The key is copied into the 1^{st} 4 words of the expanded key.
3. In the expanded key each added word $W[i]$ depends on $W[i-1]$ and $W[i-4]$.
4. If i is a multiple of 4 then

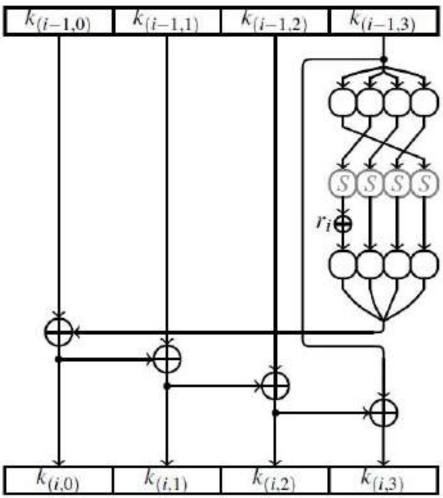
$$W[i] = SubWord(RotWord(W[i-1])) \oplus Rcon[i/4] \oplus W[i-4],$$

   where $Rcon[1] = 1$, $Rcon[j] = 2 * Rcon[j-1]$

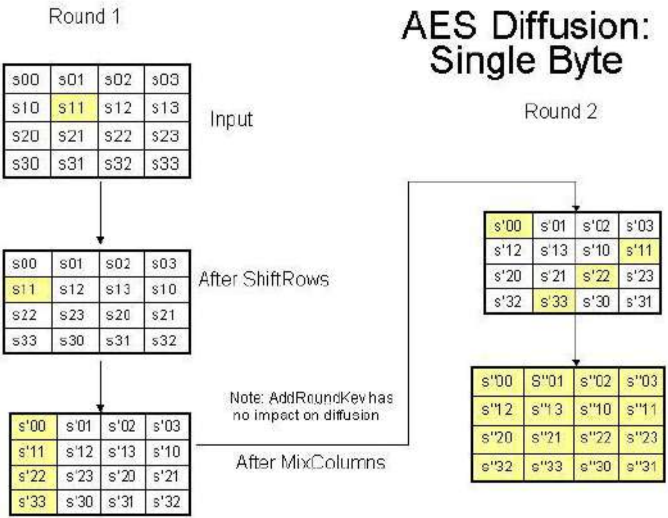
5. Else

$$W[i] = W[i-1] \oplus W[i-4].$$

Key Schedule



AES Diffusion



Design Criteria of S-Box

S-Box is defined over $GF(2^8)$ in the following way

$$y = SBox(x) = \mathbf{A} * x^{-1} + \mathbf{c}, \text{ where}$$

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathbf{c} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Recommended Block Ciphers (ENISA – Nov 2014)

Primitive	Recommendation: Legacy	Recommendation: Future
AES	✓	✓
Camellia	✓	✓

Recommended Block Ciphers (ENISA – Nov 2014)

Primitive	Recommendation Legacy	Recommendation Future
AES	✓	✓
Camellia	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
$Blow^{\geq 80-bit\ keys}$	✓	✗

Recommended Block Ciphers (ENISA – Nov 2014)

Primitive	Recommendation: Legacy	Recommendation: Future
AES	✓	✓
Camellia	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
$Blow^{\geq 80-bit\ keys}$	✓	✗
DES	✗	✗

Recommended Block Ciphers (ENISA – Nov 2014)

Primitive	Recommendation: Legacy	Recommendation: Future
AES	✓	✓
Camellia	✓	✓
Three-Key-3DES	✓	×
Two-Key-3DES	✓	×
Kasumi	✓	×
$Blow^{\geq 80-bit\ keys}$	✓	×
DES	×	×

https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

Recommended Block Ciphers

Legacy ×	Attack exists or security considered not sufficient. Mechanism should be replaced in Fielded products as a matter of urgency.
Legacy ✓	No known weaknesses at present. Better alternatives exist. Lack of security proof or limited key size.
Future ✓	Mechanism is well studied (often with security proof). Expected to remain secure in 10-50 year lifetime.

What's Removed in TLS1.3?

What's Removed in TLS1.3?

- **Key Exchange:**
  - RSA
- **Encryption algorithms:**
  - RC4, 3DES, Camellia.
- **Cryptographic Hash algorithms:**
  - MD5, SHA-1.
- **Cipher Modes:**
  - AES-CBC

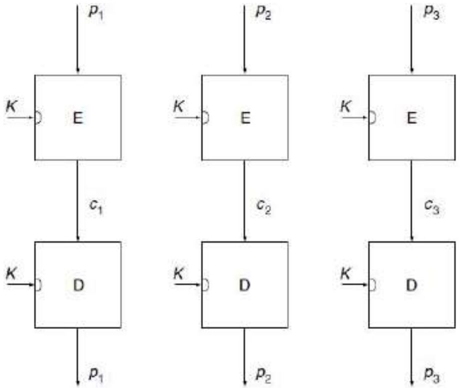
Outline

1. Introduction
2. Feistel Network
   - DES
3. SPN
   - AES
4. Modes of Operation

Recommendation of Modes of Operation

- A NIST standard FIPS 800-38A (since 2001)
- This recommendation defines five confidentiality modes of operation for use with an underlying symmetric key block cipher algorithm:
  - Electronic Codebook (ECB),
  - Cipher Block Chaining(CBC),
  - Cipher Feedback (CFB),
  - Output Feedback (OFB), and
  - Counter (CTR).
- Addendum to NIST Special Publication 800-38A for three variants of **ciphertext stealing** for CBC Mode in 2010.

Electronic Code Book (ECB) Mode



Encryption : $c_i = E_K(p_i)$, **Decryption** : $p_i = D_K(c_i)$

Properties of ECB

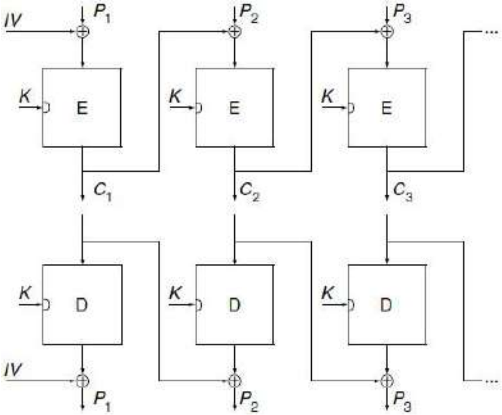
- **Advantages**
  1. No block synchronization between sender and receiver is required.
  2. Bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks.
  3. Block cipher operating can be parallelized for high-speed implementations.
- **Disadvantages**
  1. Identical plaintexts result in identical ciphertexts.
  2. An attacker recognizes if the same message has been sent twice.
  3. Plaintext blocks are encrypted independently of previous blocks.
  4. An attacker may reorder ciphertext blocks which results in valid plaintext.

Properties of ECB

- **Advantages**
  1. No block synchronization between sender and receiver is required.
  2. Bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks.
  3. Block cipher operating can be parallelized for high-speed implementations.
- **Disadvantages**
  1. Identical plaintexts result in identical ciphertexts.
  2. An attacker recognizes if the same message has been sent twice.
  3. Plaintext blocks are encrypted independently of previous blocks.
  4. An attacker may reorder ciphertext blocks which results in valid plaintext.

ECB is insecure and you should not use it!

Cipher Block Chaining (CBC)Mode

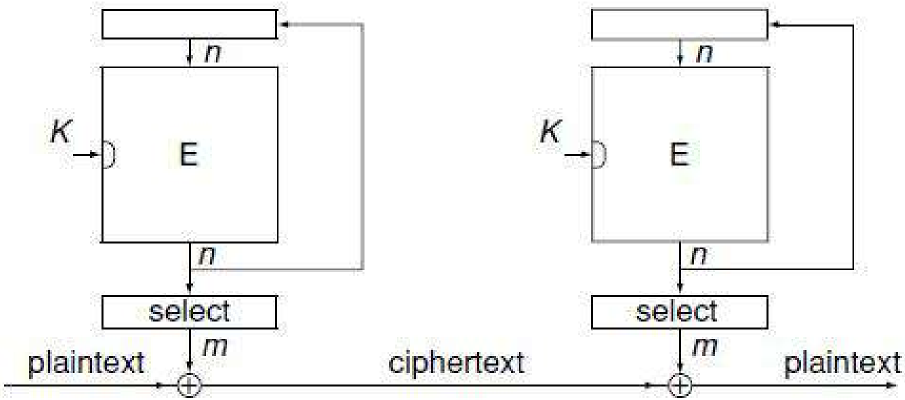


Encryption : $c_i = E_K(p_i \oplus c_{i-1})$, **Decryption** : $p_i = D_K(c_i) \oplus c_{i-1}$

Properties of CBC

- The encryption of all blocks are chained together.
- The encryption is randomized by using an initialization vector $\mathcal{IV}$.
- A single bit error in ciphertext block c_i affects decipherment of blocks c_i and c_{i+1}.
  - Block p_i' recovered from c_i is typically totally random, while the recovered plaintext p_{i+1}' has bit errors precisely where c_i did.
- Decryption can be much faster than encryption due to parallelism.
- Padding oracle attack is possible in CBC mode.

Output FeedBack (OFB) Mode

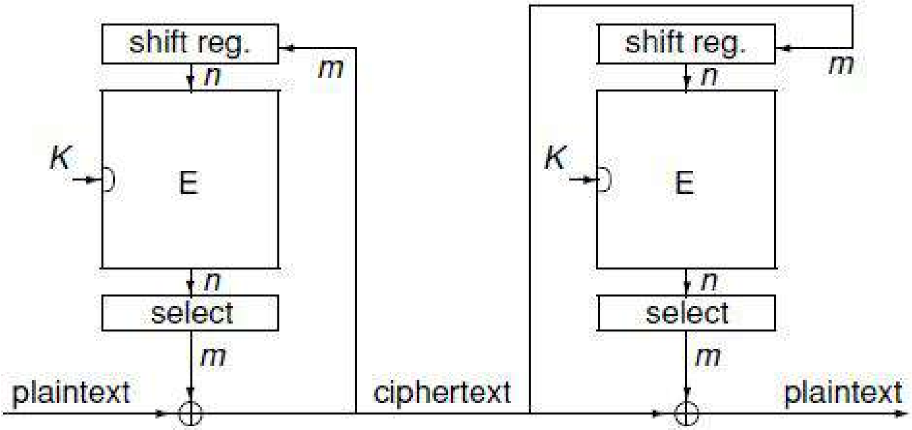


Encryption : $c_i = p_i \oplus E_K(k_{i-1})$, **Decryption** : $p_i = c_i \oplus E_K(k_{i-1})$

Properties of OFB

- It is used to build a synchronous stream cipher from a block cipher.
- The key stream is not generated bitwise but instead in a blockwise fashion.
- One or more bit errors in any ciphertext block c_i affects the decipherment of only that block.
- The $\mathcal{IV}$, which need not be secret, must be changed if an OFB key K is re-used.

Cipher FeedBack (CFB) Mode

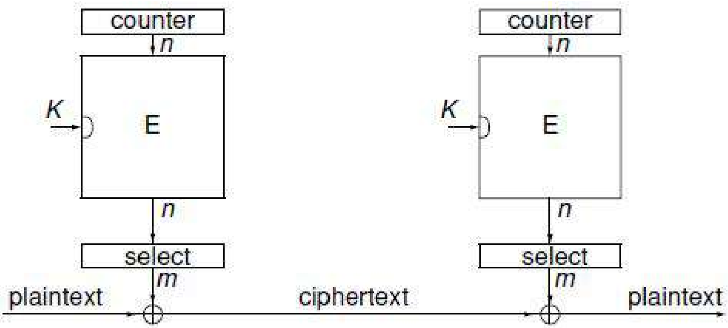


Encryption : $c_i = p_i \oplus E_K(c_{i-1})$, **Decryption** : $p_i = c_i \oplus E_K(c_{i-1})$

Properties of CFB

- Since the encryption function E_K is used for both CFB encryption and decryption, the CFB mode must not be used if the block cipher E is a public-key algorithm.
- The CFB mode may be modified
  - to allow processing of plaintext blocks whose size is less than the size of the feedback variable.
- It can be used in situations where short plaintext blocks are to be encrypted.

CounTeR (CTR) Mode



Encryption : $c_i = p_i \oplus E_K(Nonce \| CTR)$

Decryption : $p_i = c_i \oplus E_k(Nonce \| CTR)$

Properties of CTR

- It uses a block cipher as a *stream cipher*
- The key stream is computed in a blockwise fashion
- Unlike CFB and OFB modes, the CTR mode can be parallelized – desirable for high-speed implementations, e.g., in network routers

Galois Counter Mode (GCM)

- AES-GCM Authenticated Encryption (proposed by D. McGrew & J. Viega)
  - Designed for high performance (Mainly with a HW viewpoint)
  - This is used for authenticated encryption with associated data (AEAD), and its specialization, GMAC, for generating a MAC on data that is not encrypted.
  - A NIST standard FIPS 800-38D (since 2007)
  - Included in the NSA Suite B Cryptography, IPsec (RFC 4106), IEEE P1619, TLS 1.2, TLS1.3

Galois Counter Mode (GCM)

- AES-GCM Authenticated Encryption (proposed by D. McGrew & J. Viega)
  - Designed for high performance (Mainly with a HW viewpoint)
  - This is used for authenticated encryption with associated data (AEAD), and its specialization, GMAC, for generating a MAC on data that is not encrypted.
  - A NIST standard FIPS 800-38D (since 2007)
  - Included in the NSA Suite B Cryptography, IPsec (RFC 4106), IEEE P1619, TLS 1.2, TLS1.3
- **How it works:**

Galois Counter Mode (GCM)

- AES-GCM Authenticated Encryption (proposed by D. McGrew & J. Viega)
  - Designed for high performance (Mainly with a HW viewpoint)
  - This is used for authenticated encryption with associated data (AEAD), and its specialization, GMAC, for generating a MAC on data that is not encrypted.
  - A NIST standard FIPS 800-38D (since 2007)
  - Included in the NSA Suite B Cryptography, IPsec (RFC 4106), IEEE P1619, TLS 1.2, TLS1.3
- **How it works:**
  - Encryption is done with AES in CTR mode
  - Authentication tag computations : “Galois Hash"
    - A Carter-Wegman-Shoup universal hash construction: polynomial evaluation over a binary field
    - Uses $GF(2^{128})$ defined by the “lowest" irreducible polynomial

$$g(x) = x^{128} + x^7 + x^2 + x + 1$$

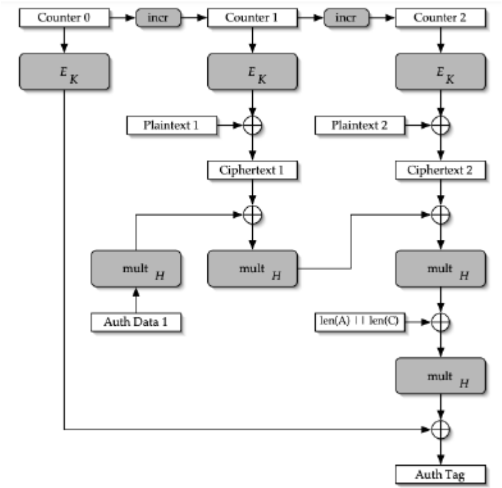
Galois Counter Mode (GCM)

- AES-GCM Authenticated Encryption (proposed by D. McGrew & J. Viega)
  - Designed for high performance (Mainly with a HW viewpoint)
  - This is used for authenticated encryption with associated data (AEAD), and its specialization, GMAC, for generating a MAC on data that is not encrypted.
  - A NIST standard FIPS 800-38D (since 2007)
  - Included in the NSA Suite B Cryptography, IPsec (RFC 4106), IEEE P1619, TLS 1.2, TLS1.3
- **How it works:**
  - Encryption is done with AES in CTR mode
  - Authentication tag computations : "Galois Hash"
    - A Carter-Wegman-Shoup universal hash construction: polynomial evaluation over a binary field
    - Uses $GF(2^{128})$ defined by the "lowest" irreducible polynomial

$$g(x) = x^{128} + x^7 + x^2 + x + 1$$

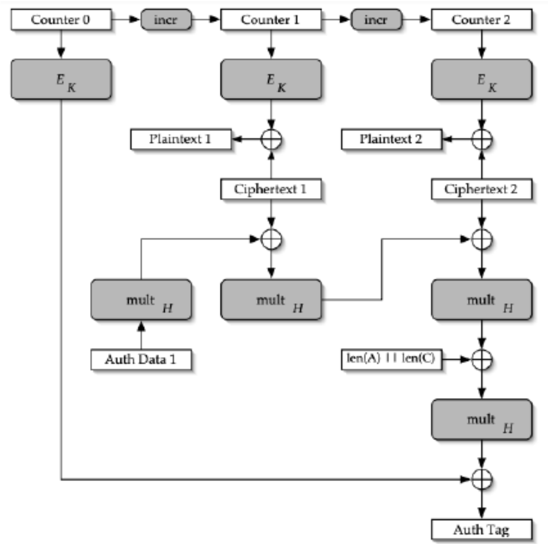
    - Computations based on $GF(2^{128})$ arithmetic

Galois Counter Mode (GCM) Encryption



$mult_H$ denotes multiplication in $GF(2^{128})$ by the hash key $H = E_K(0^{128})$

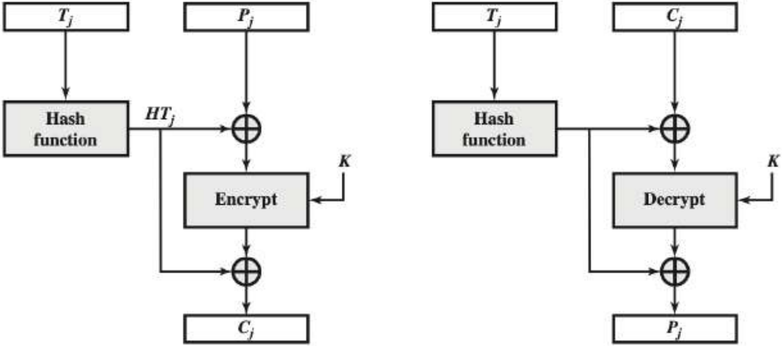
GCM Decryption



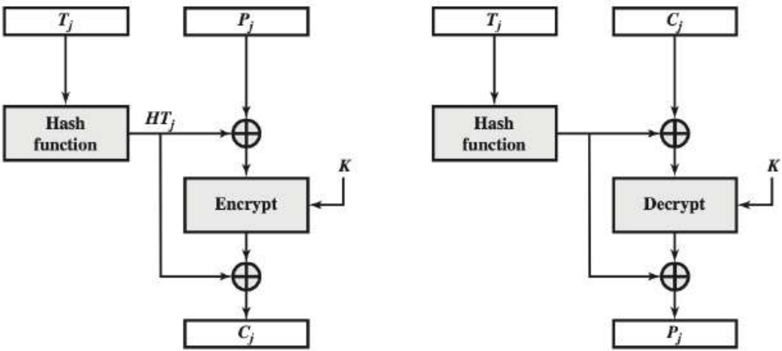
XTS-AES Mode

- NIST approved XTS-AES algorithm a mode of operation of the AES algorithm published in 2010 (Std. IEEE 1619-2007).
- **XTS** stands for the **X**EX **T**weakable Block Cipher with Ciphertext **S**tealing
- It was designed for the cryptographic protection of data on storage devices (data at rest).
- It has received widespread industry support.
- It is based on the concept of tweakable block cipher.
- The form of this concept used in XTS-AES was first described by Phillip Rogaway in 2004.

Tweakable Block Cipher



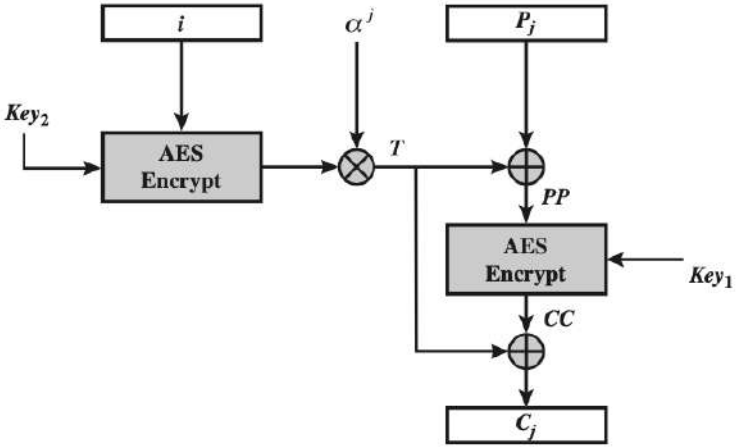
Tweakable Block Cipher



William Stallings,
Cryptography and Network Security: Principles and Practice, Pearson Education Canada, 2020.

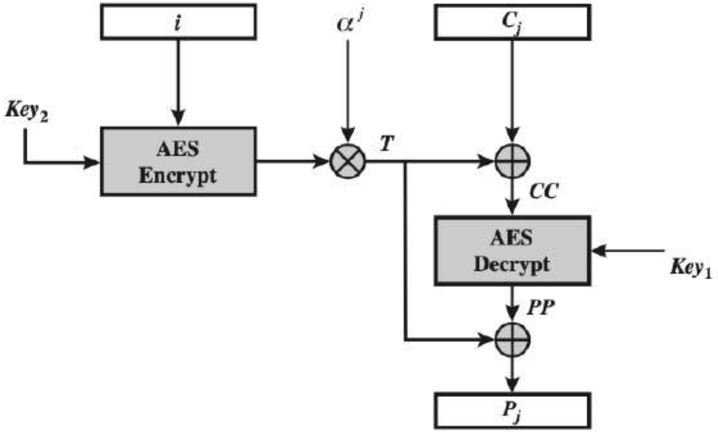
XTS-AES Mode

Encryption



XTS-AES Mode

Decryption



The End

Thanks a lot for your attention!