CISSP® Common Body of Knowledge Review:

Cryptography Domain – Part 1

Version: 5.9.2

Learning Objective

Cryptography Domain

The Cryptography domain addresses the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authentication.

The candidate is expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and non-repudiation of the parties involved; and the organization and management of the Public Key Infrastructure (PKIs) and digital certification and management.

Reference: *CISSP CIB*, January 2012 (Rev. 5)

Cryptography Domain – Part 1

- Terms, Definition
- Cipher Types
  - Classic Ciphers
  - Modern Ciphers
- Cryptographic Algorithms
  - Hash Function Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Hybrid Cryptography

Cryptography Domain – Part 2

- Utilization of cryptography
  - Public Key Infrastructure (PKI)
  - HTTP, S-HTTP, IPsec, SSH, SET
  - Single Sign-On (SSO)
  - Secured E-mail
- Types of crypto attacks
  - Crypto-analytic Attacks
  - Cryptographic Attacks
- Discussion on export of crypto technologies

Concept

Security Principles and Cryptography

Objectives of Cryptography:

- Confidentiality – unauthorized persons cannot access information.
- Integrity – ensures the message remains unmodified.

Cryptography provides:

- Confidentiality – Encryption.
- Integrity – Hash/Message Digest.
  - Authentication – to verify the identity of a subject.
  - Non-repudiation – sender can't deny sending.

Stuff To Look Out For…

- Authentication – Is NOT part of the "C.I.A. Triad".

Cryptograph ... (1/3)

- Cryptography – the science of secret writing.
- Cryptology – the study of cryptography and cryptanalysis.

- Cryptosystem – hardware and/or software implementation of cryptography.
- Algorithm – a precise rule (or set of rules) specifying how to solve some problem or accomplish a specific task.
- Cipher – cryptographic transformation operating with bits or characters.

Cryptograph … (2/3)

- Plaintext/Cleartext – data in unscrambled form.
- Ciphertext/Cryptogram – scrambled data.

- Encipher/Encrypt/Encode – act of scrambling using key.
- Decipher/Decrypt/Decode – descrambling with key.

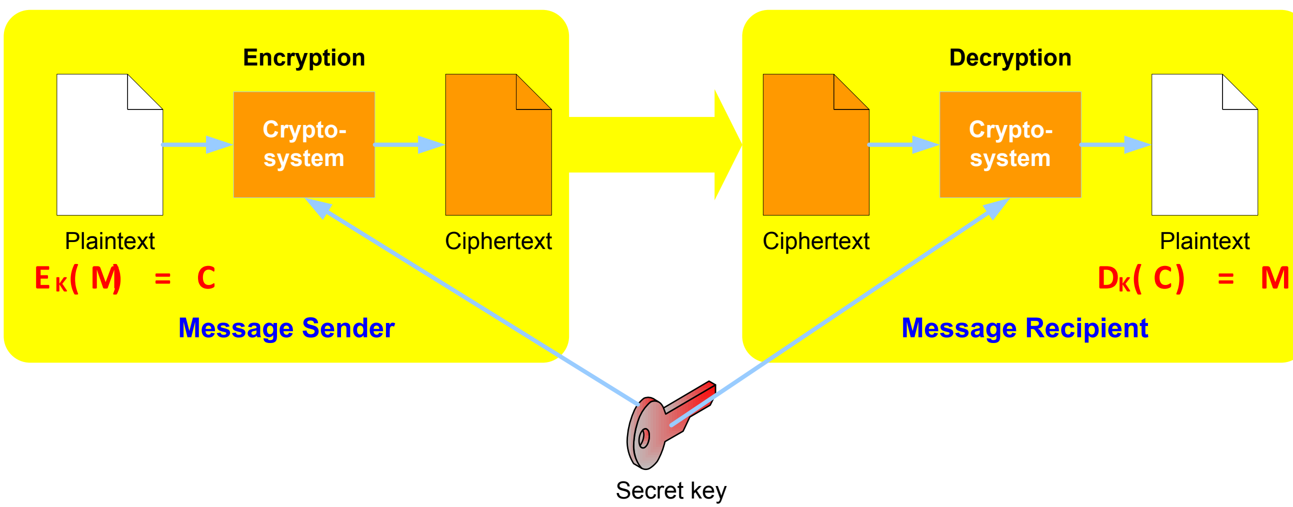
- Cryptanalysis – the practice of breaking cryptosystems or obtaining plaintext from cipher text without a key.
- Work Factor – time, effort, and resources necessary to break a cryptosystem.

Cryptograph … (3/3)

- Key – For crypto, a secret value in the form of a sequence of characters used to encrypt and decrypt.
- Key clustering – instance where two keys generate the same ciphertext from same plaintext.
- Keyspace – All possible values used to construct keys. The larger keyspace the better.
- Initialization Vector (IV) – In crypto, IV is a block of bits used as the initializing input algorithm for the encryption of a plaintext block sequence.
  - IV increases security by introducing additional cryptographic variance and to synchronize cryptographic equipment

Cryptographic Algorithm & Operation

- Cryptographic algorithm – A set of mathematical function and rules that takes plaintext and a key as input, and product ciphertext as output.
- Cryptographic operation – Encryption/Decryption
  - Encryption – An act to convert plaintext into ciphertext in order to preserve confidentiality of data.
  - Decryption – An act to convert ciphertext back to plaintext.



Strength of Encryption

- The goal of the cryptosystem is to make compromising it too expensive or time consuming to justify the effort.

- The strength of the encryption method comes from:
  1. The algorithm
  2. Secrecy of the key
  3. Length of the key
  4. Initialization vectors (IV)
  5. And how they all work together (encryption method)

- Strength (a.k.a. work factor) refers to how hard it is to figure out the algorithm or a key (whichever is not made public) used in the cryptosystem.
  – "Work Factor" is an estimate of the effort it would take an attacker to compromise the encryption method.

Cryptography Domain – Part 1

- Terms, Definition
- Cipher Types
  - Classic Ciphers
  - Modern Ciphers
- Cryptographic Algorithms
  - Hash Function Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Hybrid Cryptography

Cipher Types

Classic Ciphers:

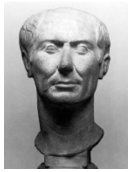
- Substitution cipher
- Transposition cipher
- Polyalphabetic (or running key) cipher

Modern Ciphers:

- Block cipher
- Stream cipher
- Steganography
- Combination: Complexity can be created by use combination above.

Substitution Cipher

- A substitution cipher substitutes one piece of information for another.
  - This is most frequently done by offsetting letters of the alphabet. (a.k.a. “shift alphabet”)
- Two examples are:
  - Caesar cipher
  - ROT13 cipher on UNIX



Confederacy’s cipher disk

ABCDEFGHIJKLMNOPQRSTUVWXYZ

and sliding everything up by 3, you get

ABCDEFGHIJKLMNOPQRSTUVWXYZABC

so “D = A”, “E = B”, “F = C”, and so on.

Transposition Cipher

- Instead of replacing the characters with other characters, this cipher simply changes the order of the characters.
- The key determines the positions that the characters are moved to
- The key for this cipher is not standard.
  - Instead of a list of alphabetic substitutions, it is a mapping order.
  - Such as (1,2,3,4,5) = (3,4,5,2,1). This means that the third element is put in place of the first, thus followed by the fourth, then the fifth, second, and finally followed by the original first element.
  - Example: "WORLD" -> "RLDOW"

Transposition Cipher

- Permutations of this cipher run in blocked matrices. This means that the message is spread out into a matrix.
- Example: “I LOVE CISSP CBK REVIEW CLASS 2012"

ILOVECI	ICW2012
SSPCBKR	LBCLASS
EVIEWCL	OKREVIE
ASS2012	VECISSP

Polyalphabetic (or Running Key) Cipher

- The running key cipher is a type of substitution cipher
  - Invented by Blaise de Vigenère in 19th century
  - The cryptographic algorithm is polyalphabetic substitution, where the secret key is repeated along the length of plaintext/ciphertext

```
Plaintext:  COMPUTING GIVES INSIGHT
Keyword:    LUCKYLUCK YLUCK YLUCKYL
Ciphertext: NIOZSECPQ ETPGC GYMKQFE
```

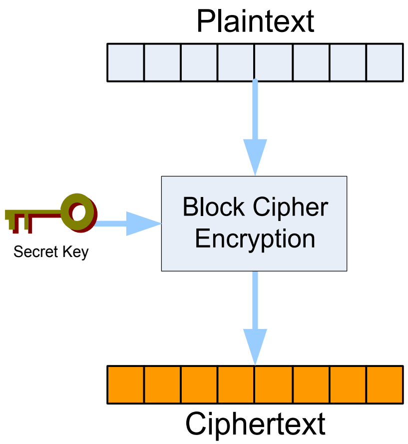
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Source: http://astro.ocis.temple.edu/~dhill001/vigenere/vigenere.html

Block Cipher

Block Cipher

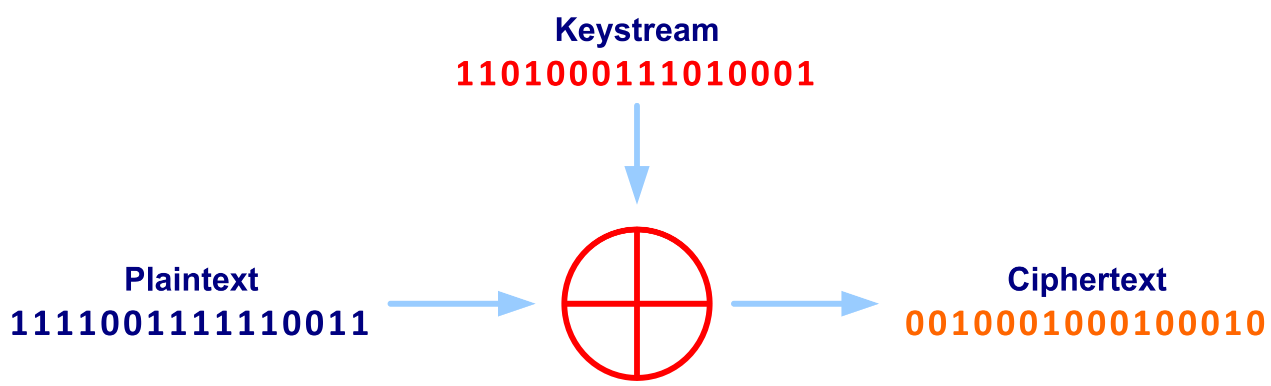
- Operate on fixed size block of plaintext.
- The encryption algorithm takes a fixed-length block of plaintext and create a block of ciphertext in the same length.
  - Usually 8-byte (64-bit)
- Usually implemented in software.
- Generally, Block cipher encryption is slower than Stream cipher encryption.
- Example: DES, Triple DES, AES, IDEA



Stream Cipher

Stream Cipher

- Operate on continuous streams of plaintext.
- Usually implemented in hardware.
- Functional complex, with long key that does not repeat.
- Statistically unpredictable.
- Keystream should NOT be linearly related to key.
- Example: RC4, SEAL, VEST



Steganography

Steganography is a method of hiding data in another media so that the data's very existence is concealed.

- Microdot, very popular in World War II
- Computer files (graphic images, MP3, or video) contain unused or insignificant areas of data… Steganography takes advantage of these areas, replacing them with information.
- The files can then be exchanged without anyone knowing what really lies inside of them.
- Can be used to insert concealed digital watermarks.

Note: For CISSP Exam… Steganography DOES NOT USE algorithms or keys to encrypt data…it hides data within another object.

Cryptography Domain – Part 1

- Terms, Definition, Concept & History
- Cipher Types
  - Classic Ciphers
  - Modern Ciphers
- Cryptographic Algorithms
  - Hash Function Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Hybrid Cryptography

Hash Function Cryptography

- A hash function takes an input of arbitrary length and outputs a fixed size value – "Hash Value".
- The maximum number of input and output bits is determined by the design of the hash function.
  - Pre-image resistance. A good hash function is "one-way". Original input (message or file) can not be derived from the hash value.
  - Collision resistance. Two inputs into a hash function should not produce the same hash value.

Hash Function Cryptography

- Cryptographic hash functions are used to provide integrity, authentication and non-repudiation.
  - Message digest, if the message or file is used as an input into a cryptographic hash function.
  - Message authentication, if a secret key is used along with a message as inputs into a cryptographic hash function.
  - Digital signature, if the private key is used as an input, and the output can be verified with the public key.

- Cryptographic hash functions are also used as "randomness extractor" for pseudo-random number generators (PRNGs)

Hash Function Cryptography

There are two flavors and a hybrid hash functions:

- Non-keyed digest (for integrity)
  - Message Integrity Code (MIC).
  - Modification Detection Code (MDC).
- Keyed digest (for authentication)
  - Message Authentication Code (MAC): Secret key + message.
  - Keyed-hash MAC or Hashed MAC (HMAC): MAC + MDC.
- Digital signature (for non-repudiation)

Popular message digest algorithms:

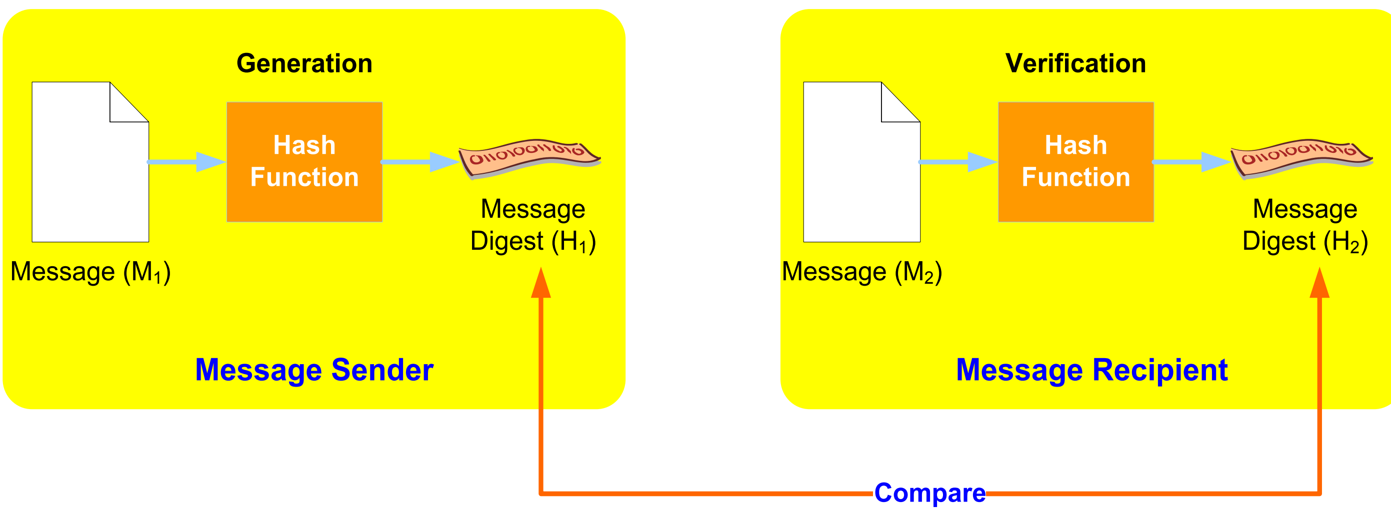
- MD5, RIPE-MD, HAVAL,
- FIPS 186-2: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.

Popular digital signature algorithms:

- ElGamal,
- FIPS 180-2: DSA, EC-DSA.

Hash Function Cryptography – Non-Keyed Digest

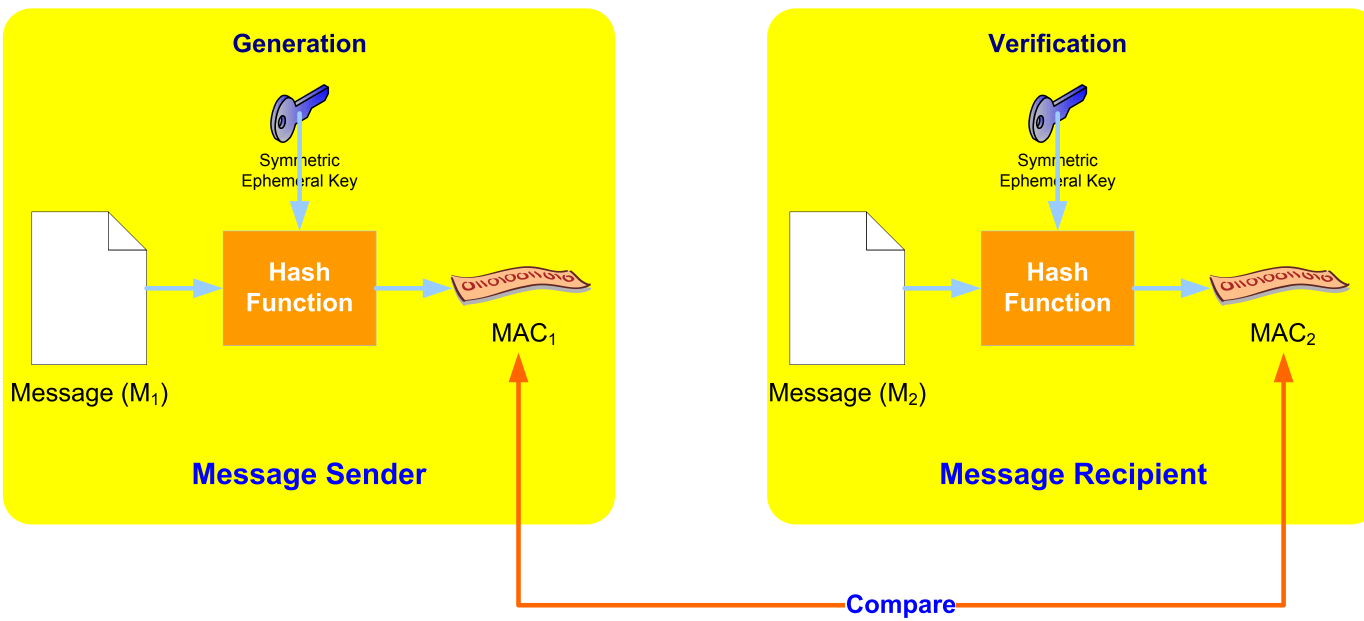
- Non-keyed digest is used to provide integrity function. The output fixed-size “hash value” is called:
  - Message Digest (MD) in cryptography world.



Hash Function Cryptography – Keyed Digest

- Keyed digest is used to provide authentication function. The output fixed-size "hash value" is called:
  - Message Authentication Code (MAC): Secret key (symmetric ephemeral key) + message.

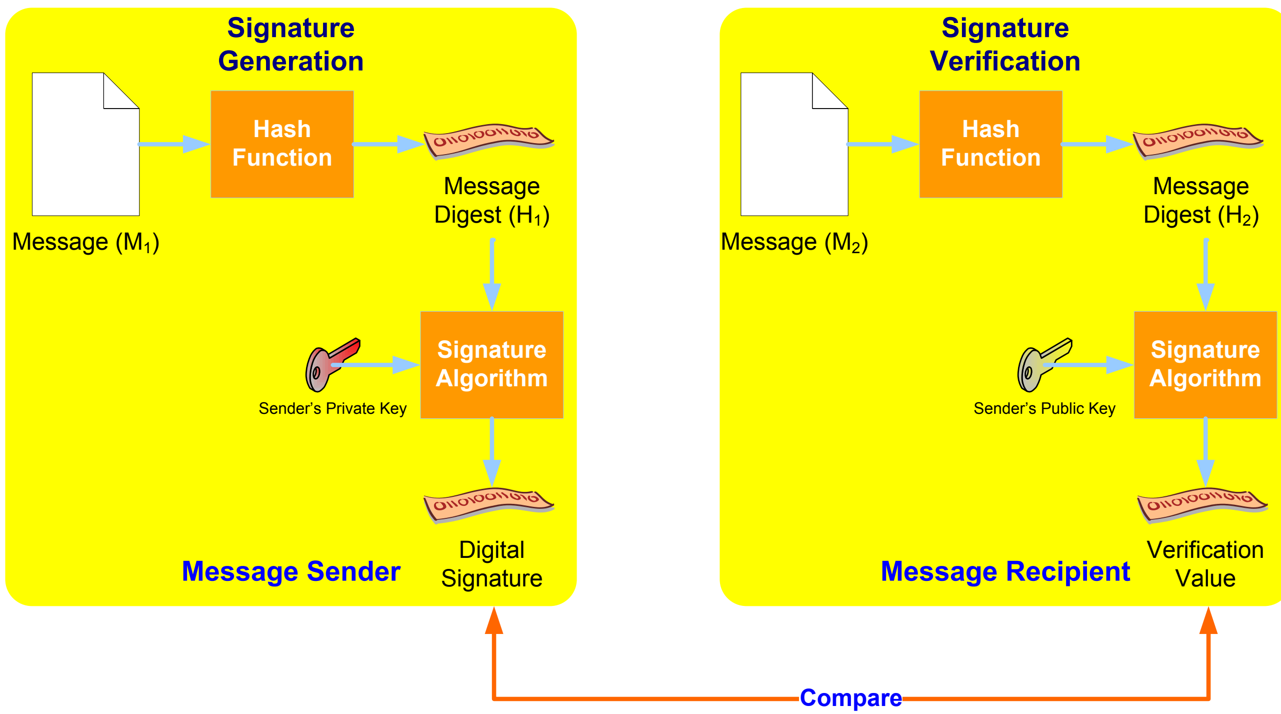
    and Keyed-Hash MAC (HMAC).)



Reference: FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 6, 2002.

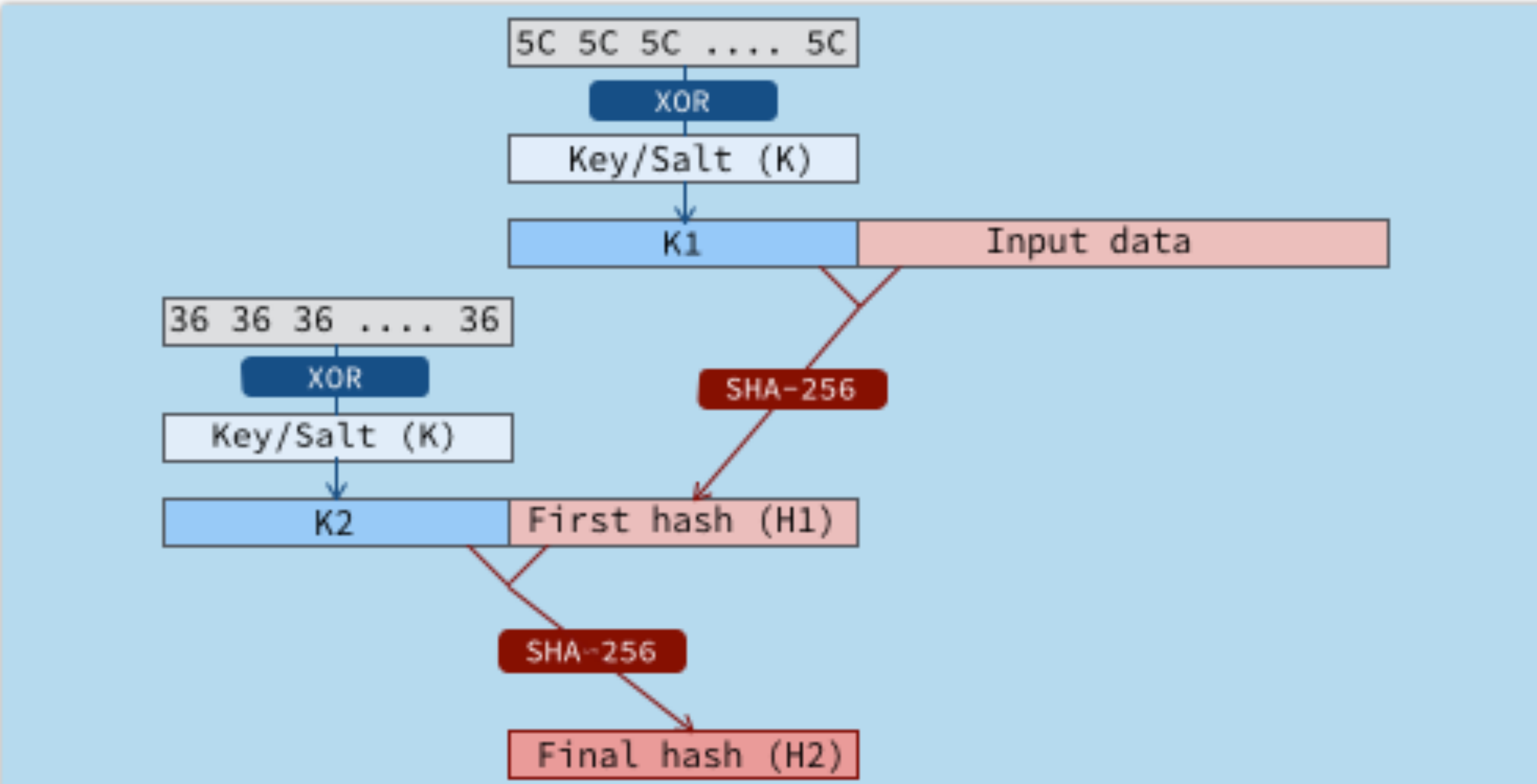
Hash Function Cryptography – Digital Signature

- Digital signature (or digital fingerprint) is used to provide non-repudiation function.
- Digital signature is a hybrid cryptography that uses non-keyed hash function and asymmetric key-pair (public key & private key).



Reference: FIPS 186-2, *Digital Signature Standard (DSS)*, January 27, 2000.

HMAC



HMAC performs two iterations of a chosen cryptographic hash to create a "keyed hash"

Hash Function Cryptography – Randomness Extractor

- True random number is hard to find, what computing machines generates is “pseudo random”

- To add “randomness”, the PRNG (pseudo-random number generator) output is put through a cryptographic hash functions

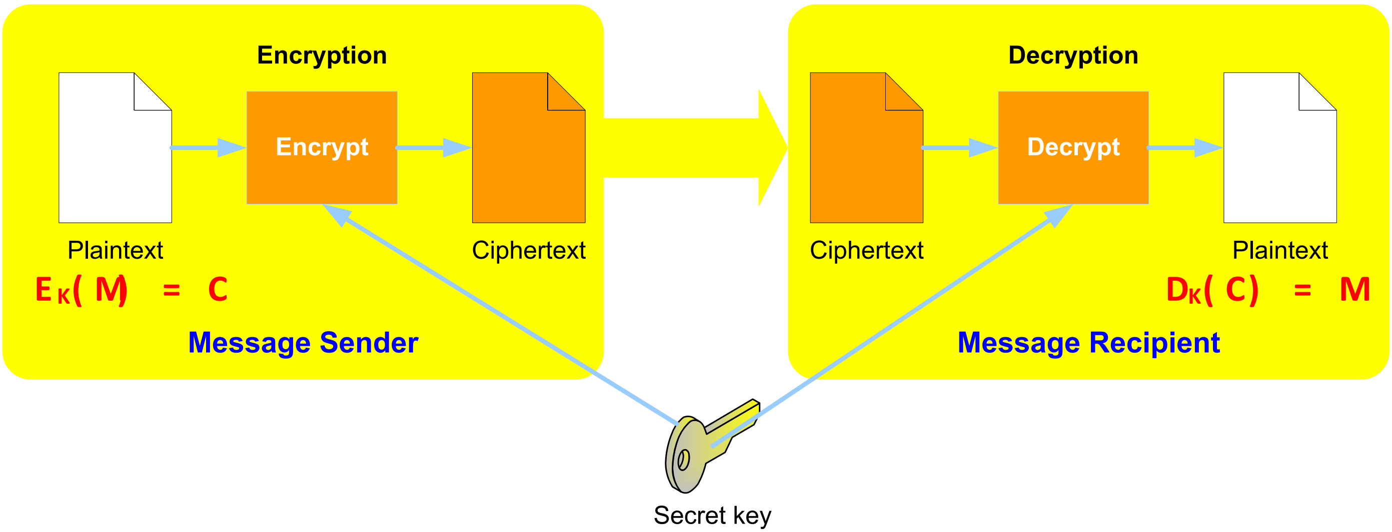
Cryptography Domain – Part 1

- Terms, Definition, Concept & History
- Cipher Types
  - Classic Ciphers
  - Modern Ciphers
- Cryptographic Algorithms
  - Hash Function Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Hybrid Cryptography

Symmetric Key Cryptography

Symmetric key cryptography involves a single secret (symmetric) key.

- Both the sender and the recipient must have the same secret key.
- It is used by the sender to encrypt the message and by the recipient to decrypt it.



Symmetric Key Cryptography

- The same secret key has to be possessed by both parties.
  - Requires a secure mechanism to deliver keys.
- Each pair of users needs a unique key.
  - Key management can be difficult as the number of users grows.
  - `n*(n-1)/2`: A user group of 100 people… 4,950 keys would be needed.
- Symmetric key cryptography provides confidentiality only. Need to combine with MAC for message integrity and authentication.
- Popular symmetric key algorithms: DES, 3DES, AES, RC6, Twofish, Blowfish, etc.

Reference: *Communication Theory of Secrecy Systems*, by Claude Shannon, 1949

Symmetric Key Cryptography – Algorithms

There are two (2) ciphers that uses symmetric key algorithms for encryption:

- Block ciphers
  - Taking a fixed-length block of plaintext data and create a block of ciphertext data of same length.
- Stream ciphers
  - Generating a keystream (sequence of bits), combining the keystream with plaintext data, bit-by-bit using **XOR** operations and create a stream of ciphertext data.
  - One-time pad (a.k.a. Vernam cipher) is a type of stream cipher. The entire keystream is totally random and is used only once.

Stream Cipher – XOR Operation

- Exclusive-OR (XOR) is an operation that is applied to two bits.
- It is a function in binary mathematics
  - if both bits are the same, the result is zero (0)

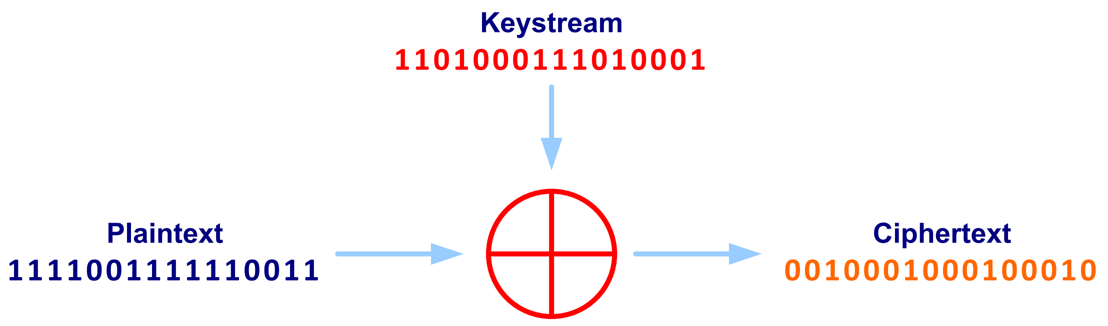
$$0 \oplus 0 = 0$$

$$1 \oplus 1 = 0$$

  - If both bits are different, the result is one (1)

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$



Stream Cipher – XOR Operation

Message	XOR	01011010	=> ASCII "Z"
Keystream		01100011	=> ASCII "c"
Ciphertext		00111001	=> ASCII "9"

Ciphertext	XOR	00111001	=> ASCII "9"
Keystream		01100011	=> ASCII "c"
Message		01011010	=> ASCII "Z"

Block Cipher – Confusion vs. Diffusion

Block Ciphers use “confusion” and “diffusion” in their encryption methods:

- Confusion (pl. Mieszanie) refers to making the relationship between the key and the ciphertext as complex and involved as possible. Thanks to this it is difficult to find relation between statistics of plaintext and ciphertext.
- Diffusion (pl. Rozpraszanie) refers to the property that modification of one bit of plaintext influence a lot of bits in ciphertext.

Reference: *Communication Theory of Secrecy Systems*, by Claude Shannon, 1949

Block Cipher Modes of Operation

In general all block ciphers operates in five (5) modes

- Block Mode
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
- Stream Mode
  - CFB (Cipher Feed Back)
  - OFB (Output Feed Back)
  - CTR (Counter)

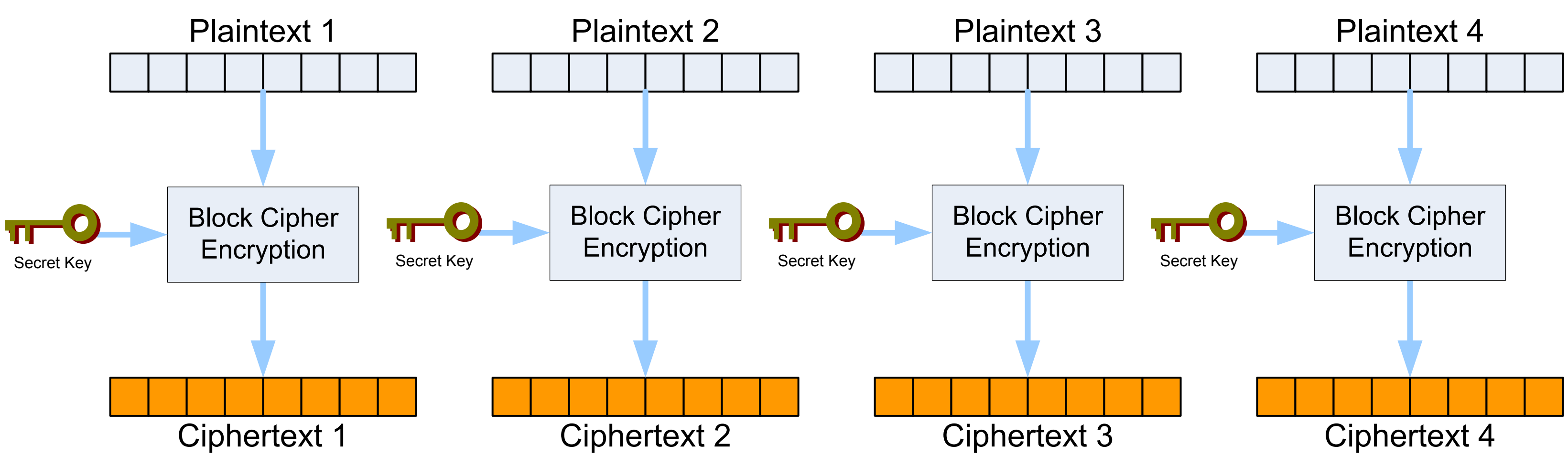
- FIPS 81 specified only 4 modes as the Federal standard, counter mode was not considered.
- NIST withdrew FIPS 81 on May 19th, 2005.

Reference: http://www.itl.nist.gov/fipspubs/withdraw.htm

Block Cipher Modes of Operation– ECB

Electronic Code Book (ECB) Block Mode

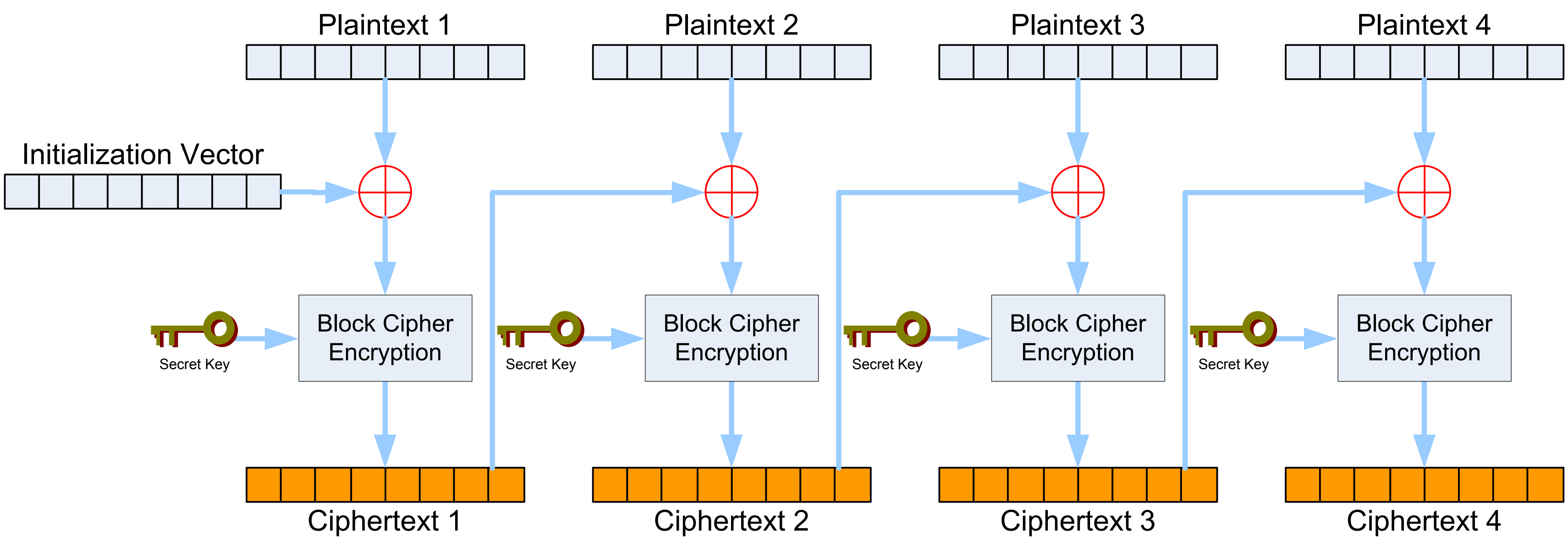
- $c_i = E_k(p_i)$
  - 64-bit data blocks processed individually, one at a time.
  - Decrypting starts at the beginning of ciphertext file and processes 64-bit block one at a time, until EOF.
- **Advantage**: Fast & Simple.
- **Disadvantage**: Susceptible to Known-plaintext attacks



Block Cipher Modes of Operation– CBC

Cipher Block Chaining (CBC) Block Mode

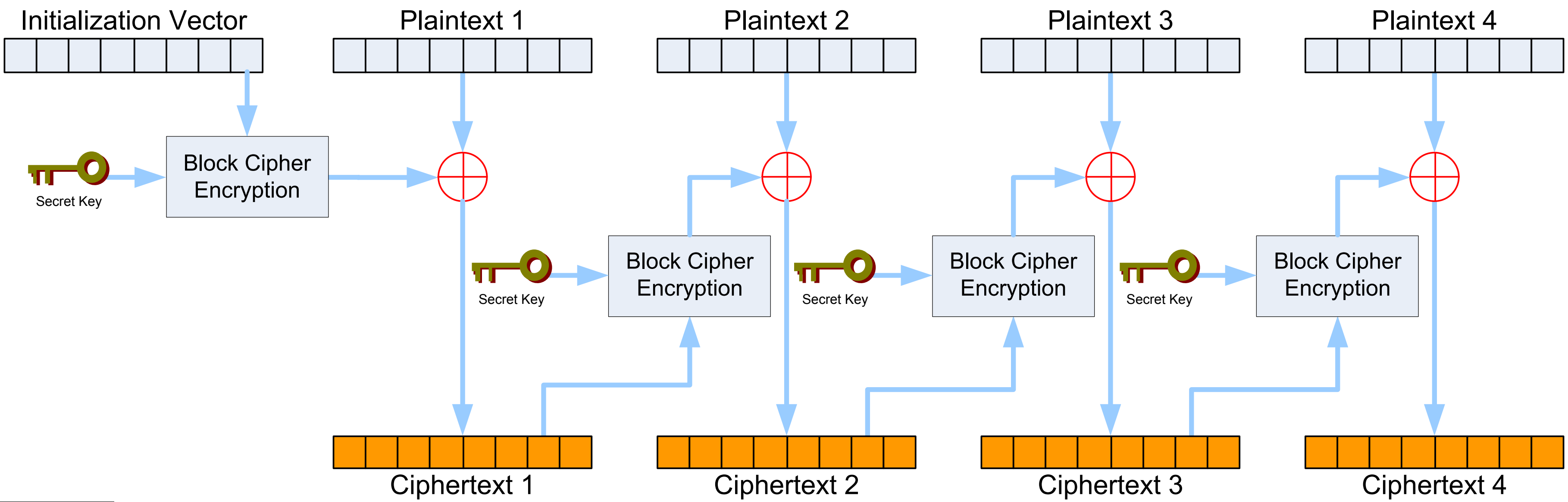
- $c_i = E_k(p_i \oplus c_{i-1})$, where: c_0 = IV
  - 64-bit plaintext blocks loaded sequentially.
  - XOR'ed with 64-bit Initialization Vector (IV).
  - Combination processed into cipher under secret key.
  - First ciphertext XOR'ed with next plaintext block.
- Most frequently used mode of operation.



Block Cipher Modes of Operation– CFB

Cipher Feed Back (CFB) Stream Mode

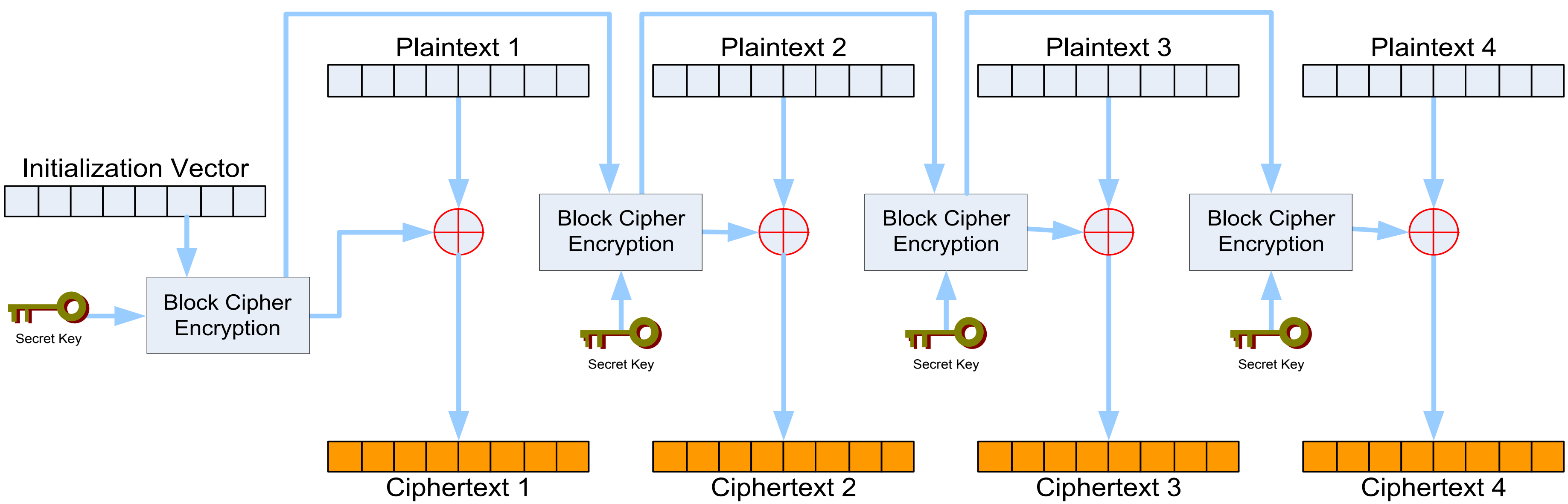
- $c_i = p_i \oplus E_k(c_{i-1})$, where c_0 = IV
  - Previous ciphertext block is encrypted and the output is combined with plaintext block using XOR to produce current ciphertext block.
  - Initialization Vector (IV) is used as a “seed” for the process.
  - Plaintext patterns are concealed by the XOR operation.



Block Cipher Modes of Operation– OFB

Output Feed Back (OFB) Stream Mode

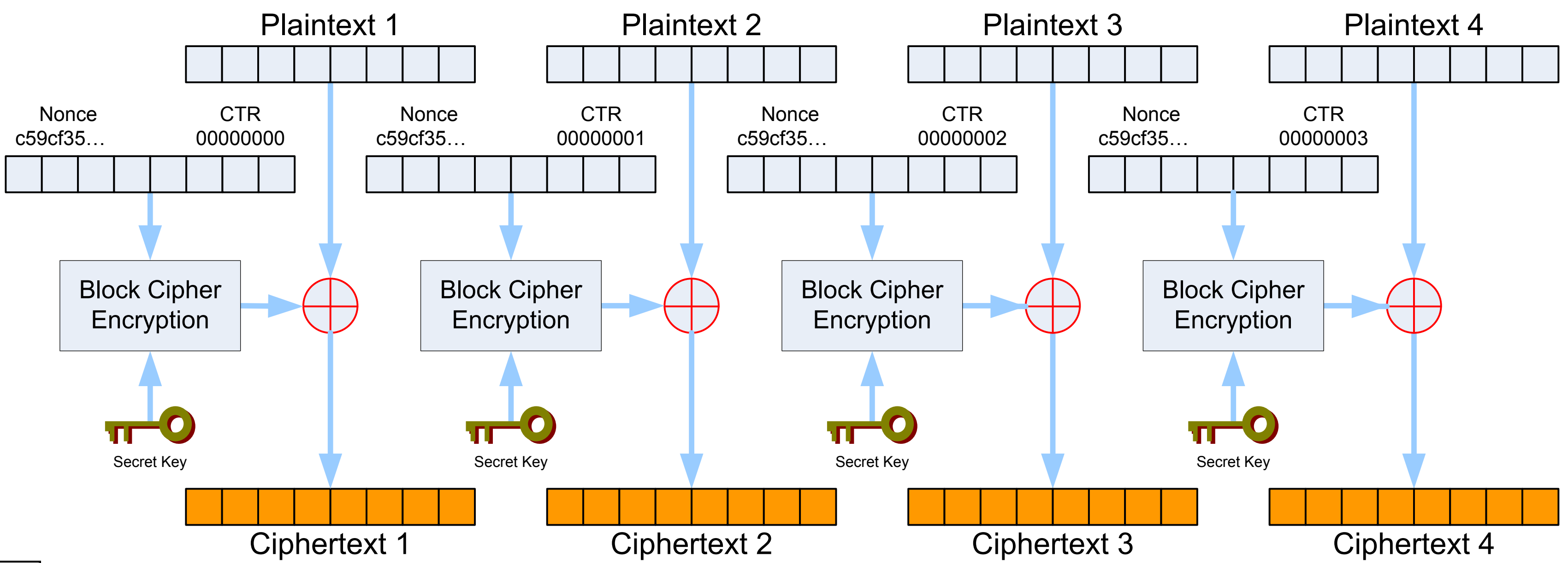
- $c_i = p_i \oplus o_i$,where: $o_i = E_k(o_{i-1})$ and o_0 = IV
  - Similar to CFB mode, except that quantity XOR'ed with each plaintext block is generated independently of both plaintext and ciphertext.
  - Initialization Vector (IV) is used as a "seed" for the process.



Block Cipher Modes of Operation– Counter

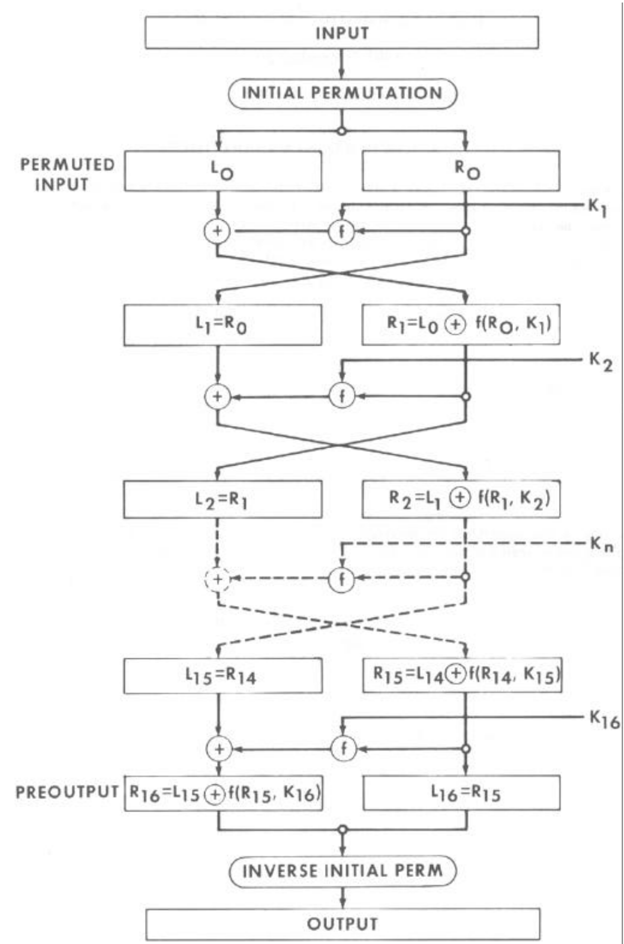
Counter (CTR) Stream Mode (Not a FIPS!)

- $c_i = p_i \oplus E_k(n_{i-1})$, where: $n_{i-1} = IV \mid t_{i-1}$
  - Similar to OFB mode the quantity XOR'ed with each plaintext block is generated independently of both plaintext and ciphertext.
  - Encrypted CTR values generate a keystream to be XOR'ed with message stream, much like stream cipher.



Symmetric Key Cryptosystem – DES …(1/2)

- Data Encryption Standard (DES), a symmetric key cryptosystem based on IBM's Lucifer cipher. DES has been a FIPS 46-1 since 1977.
- DES is a 64-bit block cipher algorithm (64-bit block = 56-bit secret key + 8-bit parity) that uses a key of 56 bits and 16 rounds of transposition and substitution to encrypt each group of 8 (64-bit) plaintext letters.



Feistel Network

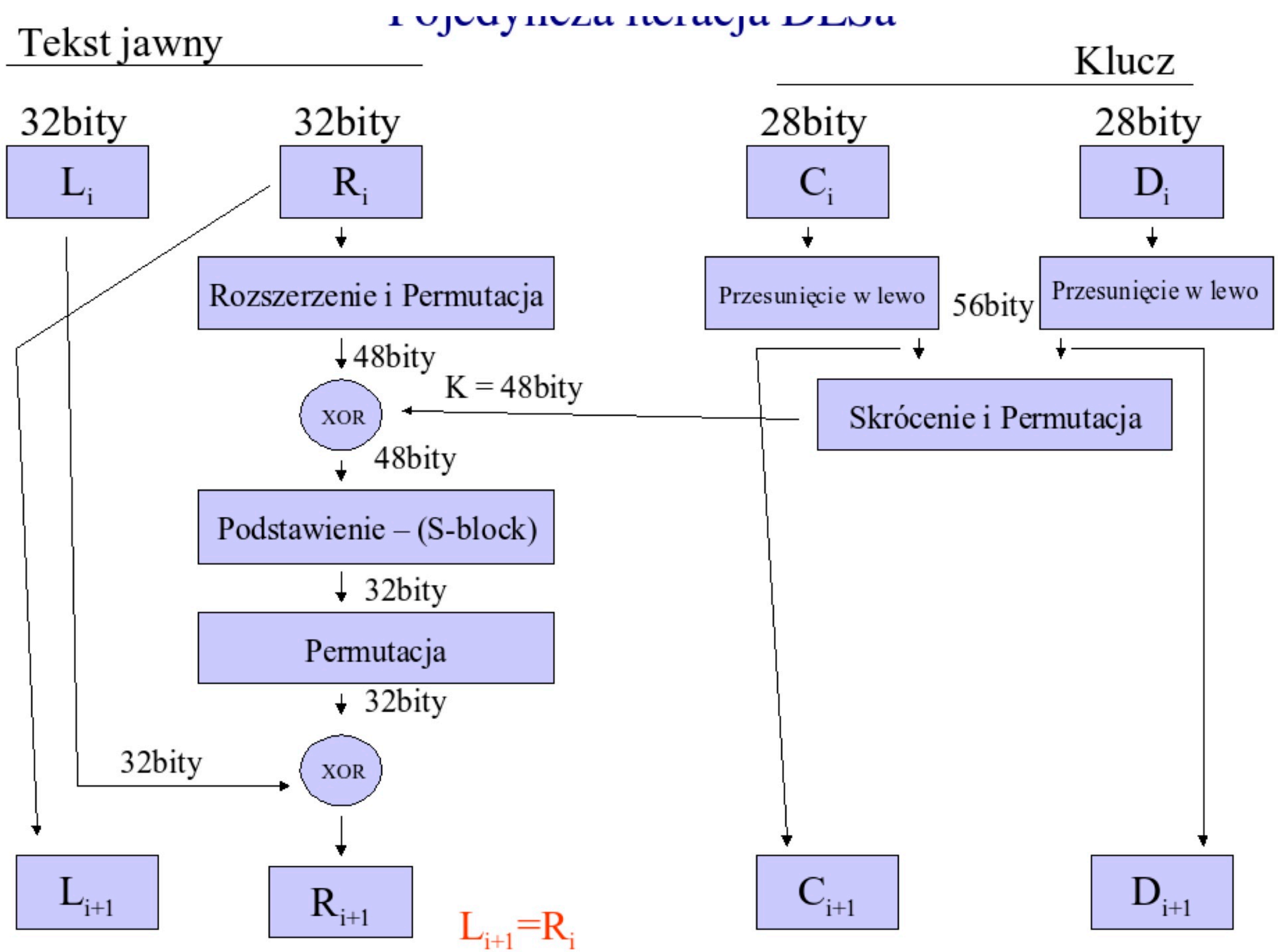
Reference:
- NIST FIPS 46-3, *Data Encryption Standard*, October 25, 1999

Symmetric Key Cryptosystem – DES …(2/2)

- For an animation of the 64-bit DES encryption process…
  - Key schedule, 56-bit key divided into two 28-bit subkeys.
    - For each successive rounds, both halves are rotated left by one or two bits.
  - Initial Permutation (IP)
    1. Permutation of a 64-bit input block to a 64-bit IP matrix
  - Rounds
    1. Expansion
    2. Key mixing
    3. Substitution
    4. Permutation

Reference: http://www.cryptool.org/en/

Symmetric Key Cryptosystem – DES …(2/2)



$L_{i+1}=R_i$

$R_{i+1}=L_i \text{ XOR } f(R_i,K_i)$

Symmetric Key Cryptosystem – DES …(2/2)

Permutacja wstępna - IP

1 2 3 4 …

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

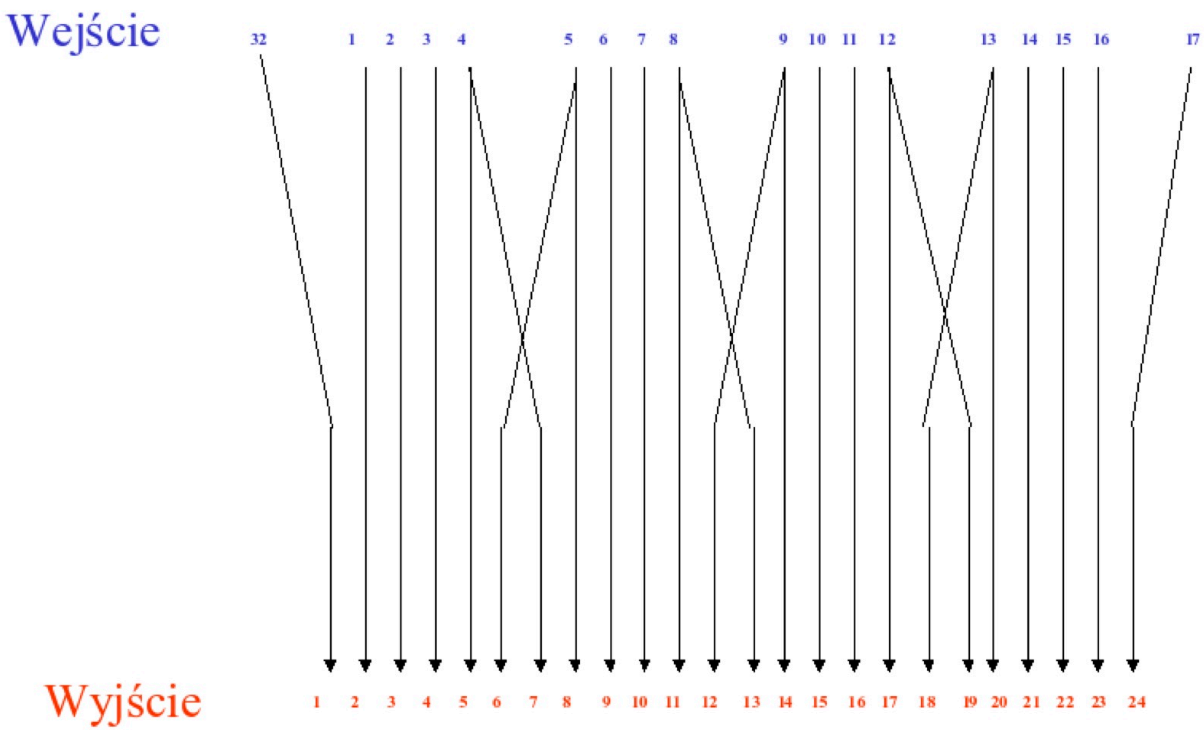
61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7

58 bit przestawiany jest na pozycję bitu nr 1 ; 50 bit na pozycję bitu nr. 2

Czytamy od lewej do prawej i z góry do dołu

Symmetric Key Cryptosystem – DES …(2/2)

Permutacja rozszerzona

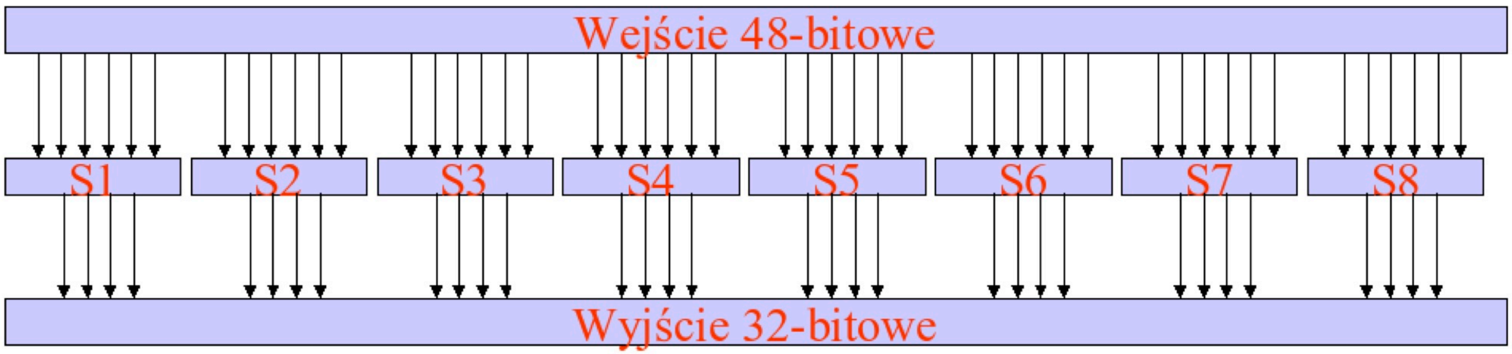


Klucz:

Permutacja z kompresją (skrócenie) – niektóre bity są pomijane.

Symmetric Key Cryptosystem – DES …(2/2)

S-block

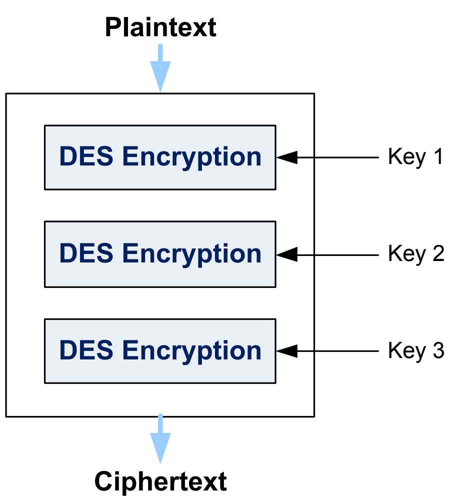


S1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Na przykład dla S1 wejście 011011 (wiersz 01 (1), kolumna 1101 (13)) daje na wyjściu 5 (0101).

Symmetric Key Cryptosystem – Triple-DES (TDES) …(1/2)

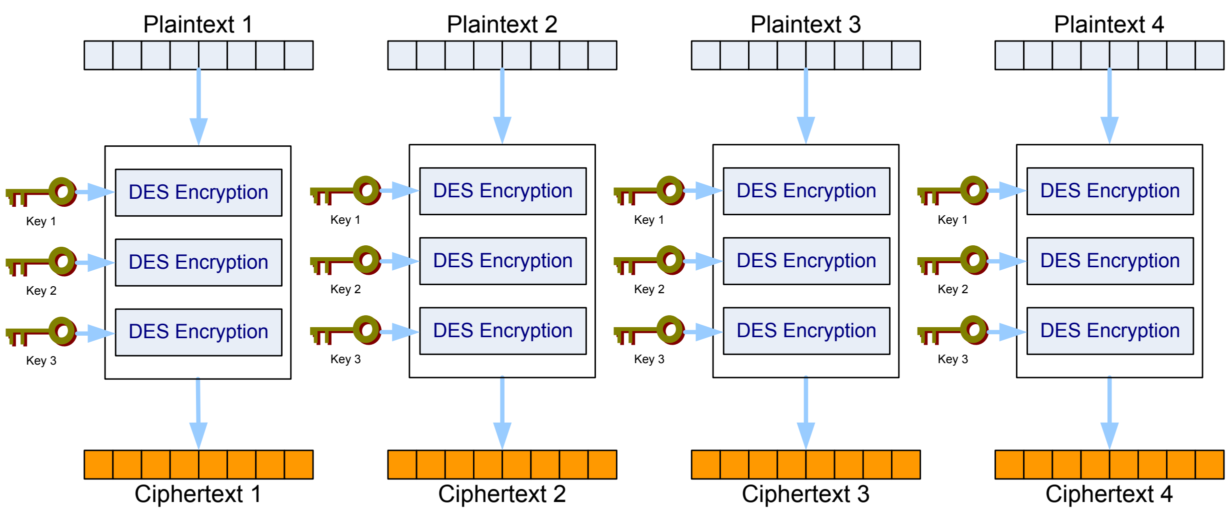
- TDES is an interim solution from NIST to provide a stronger solution than DES…
  - TDES uses 48 rounds of transposition and substitution functions in its computation.
  - TDES is approximately 2^{56} times stronger than DES.
- TDES operates in four (4) different modes…
  - DES-EEE: TDES encryption with 3 different keys
  - DES-EDE: TDES operations (encrypt-decrypt-encrypt) with 3 different keys.
  - DES-EEE2: TDES encryption with 2 different keys and 1st & 3rd operations use the same key.
  - DES-EDE2: TDES operatons (encrypt-decrypt-encrypt) with 2 different keys and 1st & 3rd operations use the same key.



Reference: NIST FIPS 46-3, *Data Encryption Standard*, October 25, 1999

Symmetric Key Cryptosystem – Triple-DES (TDES) …(2/2)

- TDES is used as the underlying block cipher algorithm for the following modes of operations:
  - Electronic Code Book (TECB in ANSI X9.52)
  - Cipher Block Chaining (TCBC, TCBC-I in ANSI X9.52)
  - Cipher Feed Back (TCFB, TCFB-P in ANSI X9.52)
  - Output Feed Back (TOFB, TOFB-I in ANSI X9.52)
  - Counter (CTR, not specified in ANSI X9.52)
- For example: TECB (TDES-EEE in ECB) …



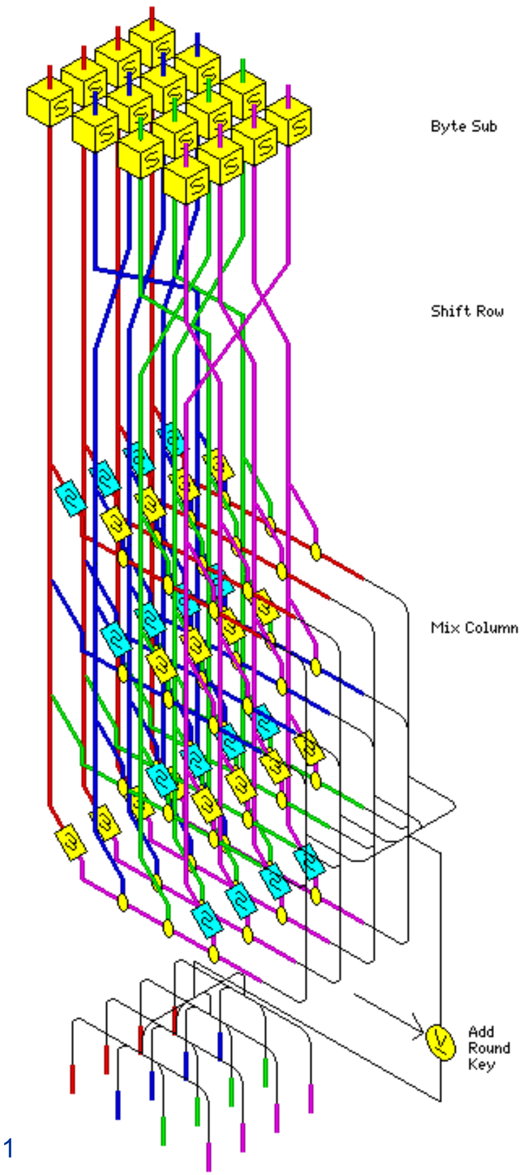
Reference:
- NIST SP 800-38A, *Recommendation for Block Cipher Modes of Operation*, December 2001.
- FIPS 46-3, *Data Encryption Standard*, October 25, 1999.

Symmetric Key Cryptosystem – Advanced Encryption Standard (AES) ... (1/4)

- NIST announced the need for a TDES replacement in 1997.
- A request for candidate symmetric block algorithms supporting key sizes of 128, 192, and 256-bit was issued.
- AES Candidates included:
  - MARS – Developed by the IBM Team that developed Lucifer (the algorithm DES was developed from).
  - RC6 – Developed by RSA.
  - Serpent – Developed by Ross Anderson, Eli Biham, and Lars Knudsen.
  - TwoFish – Developed by Counterpane Systems.
  - Rijndael – Developed by Vincent Rijmen and Joan Deamon.
  - CAST – Developed by Entrust Technologies.

Symmetric Key Cryptosystem – Advanced Encryption Standard (AES) … (2/4)

- The Rijndael algorithm developed by Vincent Rijman & Joan Daeman was selected after lengthy testing to become AES (FIPS 197)
- AES is a symmetric block cipher that can…
  - Process data blocks of 128 bits.
  - Uses cipher keys with lengths of 128, 192, and 256 bits.
  - Variable number of rounds (10 r -128 bit key, 12 r – 192 b k, 14 – 256 b k), each round containing 4 steps (Byte Sub, Shift Row, Mix Column, Add Round Key)
  - Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.



Reference:
- NIST FIPS 197, *Advanced Encryption Standard (AES)*, November 2001
- http://www.quadibloc.com/crypto/co040401.htm

Symmetric Key Cryptosystem – Advanced Encryption Standard (AES) ... (3/4)

- Like DES, AES is an block cipher algorithm for symmetric key cryptosystem.
  - Uses confusion and diffusion principles

- For both its cipher and inverse cipher, AES algorithm uses a “round function” that is composed of four different byte-oriented transformations:
  - SubByte (Confusion (pl. Mieszanie – brak zależności między kluczem i jawnym tekstem a szyfrogramem))
  - ShiftRow (Diffusion (pl. Rozpraszanie – tzw. efekt lawiny))
  - MixColumn (Diffusion)
  - AddRoundKey (Confusion)

Reference: NIST FIPS 197, *Advanced Encryption Standard (AES)*, November 2001

Symmetric Key Cryptosystem – Advanced Encryption Standard (AES) … (4/4)

- For an animation of the 128-bit AES encryption process… (http://www.formaestudio.com/rijndaelinspector/archivos/rijndaelanimation.html)
  - KeyExpansion using Rijndael's key schedule
  - Initial Round
    1. AddRoundKey
  - Rounds
    1. SubBytes
    2. ShiftRows
    3. MixColumns
    4. AddRoundKey
  - Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

Reference: http://cryptool.org/en/

Symmetric Key Cryptosystem – Other Block Ciphers

- RC5
  - Designed by Ron Rivest of RSA Security
  - Features data dependant rotations, variable block size (32,64, or 128 bits), variable key size (0 – 2040 bits), variable number of rounds
- RC6
  - Also designed by Ron Rivest. It was a candidate for AES.
  - Based on RC5, RC6 has a block size of 128 bits, supports key size of 128, 192, and 256 bits.
- Blowfish
  - Highly efficient block cipher, designed by Bruce Schneier
  - Key size: 32 – 448 bits (in steps of 8 bits)
  - 64-bit block size
  - Optimized for 32-bit micro-processors

Symmetric Key Cryptosystem – Stream Ciphers

- RC4
  - The most commonly implemented software stream cipher.
  - Used in Secure Socket Layer (SSL) and Wired Equivalent Privacy (WEP).
  - Designed by Ron Rivest of RSA Security.
  - Using pseudo-random generation algorithm.
  - Variable key size.
  - Highly efficient, much faster than any block cipher.
  - Stream ciphers can be difficult to implement correctly.

Source: http://en.wikipedia.org/wiki/RC4

Cryptography Domain – Part 1

- Terms, Definition, Concept & History
- Cipher Types
  - Classic Ciphers
  - Modern Ciphers
- Cryptographic Algorithms
  - Hash Function Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
  - Hybrid Cryptography

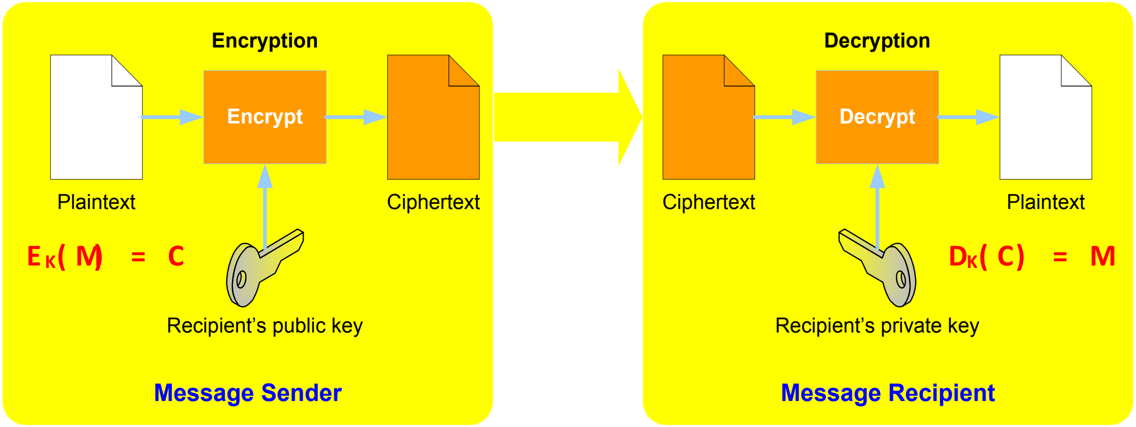
Asymmetric Key Cryptography

Asymmetric key cryptography involves two mathematically related but different keys known as a key-pair (a private key & a public key).

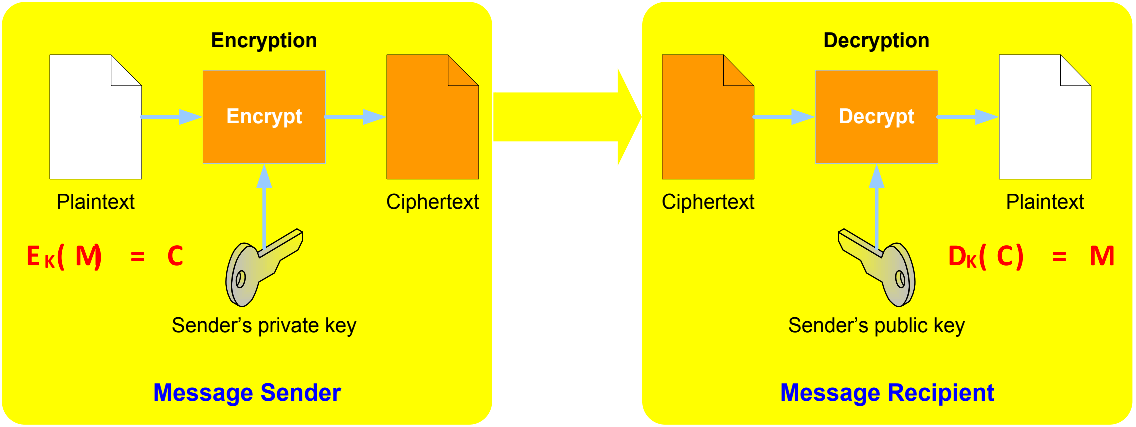
- The public key is derived from the private key.
  - Only the owner has the private key.
  - One-way mathematical link (a.k.a. "Trapdoor function").
  - The private key cannot be deduced (theoretically) by analyzing the public key.

Asymmetric Key Cryptography

- Secure message format:



- Open message format:



Asymmetric Key Cryptography – Algorithms

Asymmetric key cryptography is mathematically more complex than symmetric key cryptography.

- Factorization algorithms
- Discrete logarithm algorithms
  - Discrete Logarithm with Finite Field
  - Elliptic Curve Discrete Logarithm with Finite Field
- The public-key cryptography process is substantially slower than symmetric key cryptography process. (100 times slower in software, 1,000 to 10,000 times slower in hardware)
- Key sizes must be relatively large.

Asymmetric Key Cryptography – Factorization Algorithms

Factorization Algorithms

- Based on factoring "semi-prime" numbers (integers).
- RSA PKCS#1
  - Key generation: RSA public key and RSA private key.
  - Public-key encryption: $c = m^e \bmod n$,
    where c is ciphertext, m is message, e is RSA public exponent and n is RSA modulus.
  - Public-key decryption: $m = c^d \bmod n$,
    where d is RSA private exponent.
  - Digital signature: $m = s^e \bmod n$,
    where s is signature representative.

Reference: http://en.wikipedia.org/wiki/RSA

Asymmetric Key Cryptography – Discrete Logarithms

Discrete logarithm w/ finite field

- Based on the mathematical proof of generalized discrete logarithm problem (GDLP),
  - where computing exponentiation over a finite field is easy ($Y^x \bmod P$),
  - but computing the discrete logarithm is hard. (find x where $Y^x \equiv Z \pmod{P}$)
- Parameters have to be as large as factoring (512, 1024, 2048-bit).
- Diffie-Hellman, El Gamal, and DSA.
- Brute force attacks are infeasible against discrete logarithms. But vulnerable to chosen-ciphertext attacks.

Reference: http://en.wikipedia.org/wiki/Diffie_hellman

Asymmetric Key Cryptography – Diffie-Hellman (DH)

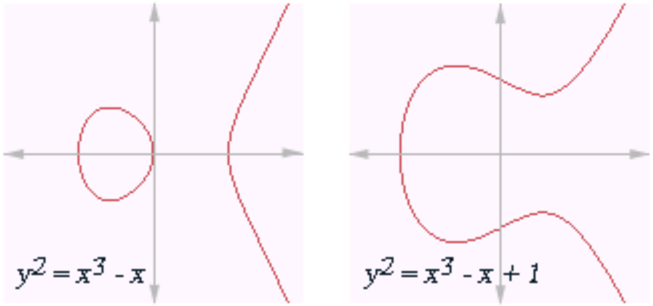
- Diffie-Hellman (DH) is a key exchange algorithm for public-key cryptography. NOT for encryption!
- DH uses finite field discrete logarithm as "trapdoor" function between private and public keys. $Y^X \pmod{P}$

Step	Alice	Exchange Methodology	Bob
1	Select Y & P with Bob	$Y^X \pmod{P}$ Public know to the world	Select Y & P with Alice
2	$Y = 11$ $P = 13$	$11^X \pmod{13}$	$Y = 11$ $P = 13$
3	Alice chooses a secret number (2)	Select a secret number	Bob chooses a secret number (5)
4	$11^2 \pmod{13}$ $121 \pmod{13} = 4$	Calculate one-way function using their secret number	$11^5 \pmod{13}$ $161051 \pmod{13} = 7$
5	Alice sends the result "4" to Bob	Send the result of the one-way function to the other person	Bob sends the result "7" to Alice
6	Calculate $7^2 \pmod{13}$ $49 \pmod{13} = 10$	Take received calculation and raise it to your secret number	Calculate $4^5 \pmod{13}$ $1024 \pmod{13} = 10$
7	Symmetric key selected through calculation is 10	Both people have the same number without revealing their "secret"	Symmetric key selected through calculation is 10

Reference: http://en.wikipedia.org/wiki/Diffie_hellman

Asymmetric Key Cryptography – Elliptic Curve Algorithm

Elliptic Curve Cryptography (ECC) uses algebraic system defined on points of elliptic curve to provide public-key cryptography.



- ECC based on the mathematical problem of factors that are coordinate pairs that fall on an elliptic curve.
- Advantages:
  - Highest strength/bit in current public-key cryptosystems.
  - Fast encryption and signature speed.
  - Small signatures & certificates. (Ideal for smart card).
- Examples:
  - ECC, EC-DH, EC-DSA, EC-ElGamal

Reference: http://en.wikipedia.org/wiki/Elliptic_curve

Asymmetric Key Cryptography – Elliptic Curve Algorithm

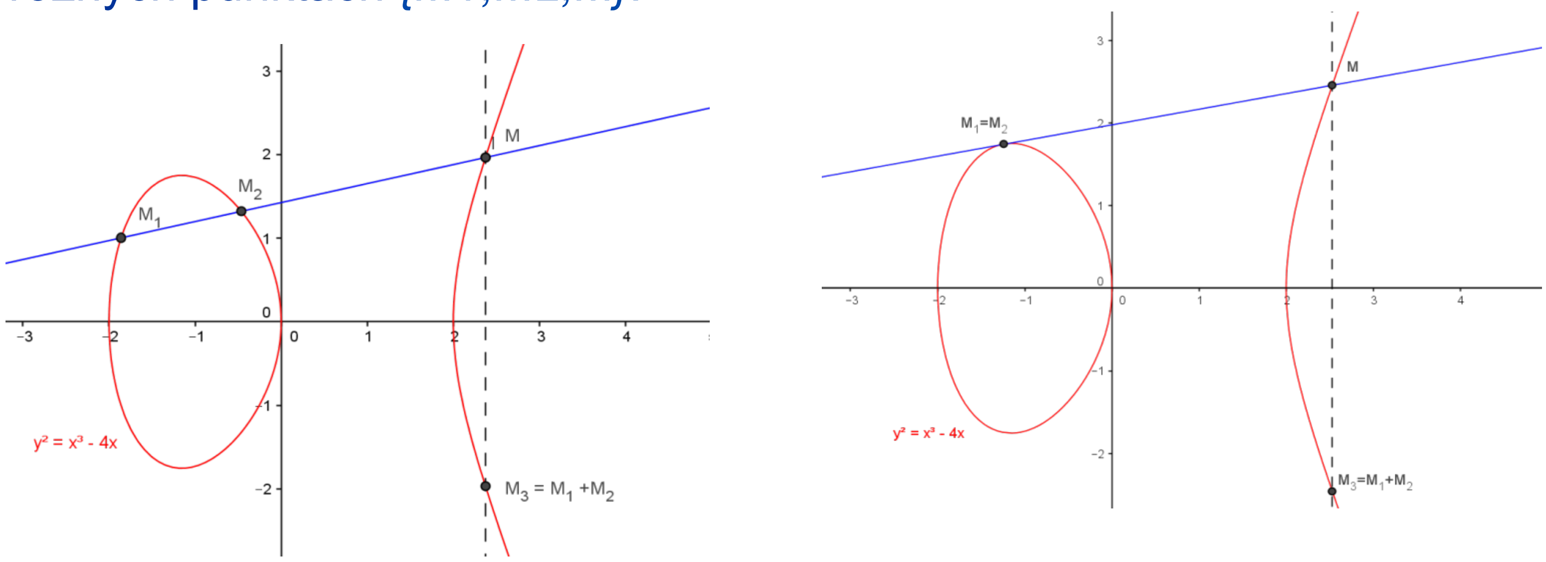
- Krzywą eliptyczną w R^2 nazwijmy zbiór rozwiązań równania Weierstrassa:

$$y^2=x^3+ax+b$$

- wraz z punktem w nieskończoności *O*, gdzie stałe *a,b* spełniają dodatkowy warunek:

$$4a^3+27b^2\neq 0$$

Dwa różne punkty *M1* i *M2*, leżące na krzywej eliptycznej, oraz przechodząca przez nie prosta przecina krzywą w dokładnie trzech różnych punktach *{M1,M2,M}.*



Reference: http://en.wikipedia.org/wiki/Elliptic_curve

Asymmetric Key Cryptography

While asymmetric key cryptography is more complex and slower than symmetric, but…

- Key management is simplified.
  - Only one party needs to know the private key.
  - Knowledge of the public key does not compromise the security of message transmissions.
- Key distribution is scalable.
  - Each subject has just one key-pair (private & public keys) .instead of **n*(n-1)/2** for symmetric key crypto.
  - Number of keys = **2*n** (1,000 users, 2,000 keys).
- Key establishment can be authenticated.
  - The key pair – private & public keys are mathematically related, but different.

Symmetric vs. Asymmetric Summary

Attribute	Symmetric	Asymmetric
Key	One shared secret key	Public/Private key pair
Key exchange	Difficult – must be done securely	Public/Private key relationship allows Public Key to be in the Open
Speed	Less complex & faster	More complex & much slower
Key Length (Bits)	Smaller (80 to 256+)	Much Larger (1024 to 2048+) *ECC (160 to 512+)
Use	Bulk encryption	Key encryption, key distribution
Security	Confidentiality/ Integrity	Confidentiality, Integrity, Authentication, Non-repudiation

Summary of Cryptography Algorithms

	Encryption	Digital Signature	Hash Function	Key Distribution
Symmetric Key Algorithms				
DES	X			
3DES	X			
AES	X			
Blowfish	X			
IDEA	X			
RC4	X			
Asymmetric Key Algorithms				
RSA	X	X		X
ECC	X	X		X
ElGamal, EC-ElGamal	X	X		X
DSA, EC-DSA		X		
Diffie-Hellman (DH), EC-DH				X
Hash Function				
RSA: MD2, MD4, MD5			X	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512			X	
HAVAL			X	

Reference: *CISSP All-in-One Exam Guide*, 4th ed.

Symmetric – Asymmetric Key Size Comparisons

Size of Symmetric Keys	
Effective Security (Bits)	**Encryption Algorithm**
80	SKIPJACK
112	3DES
128	AES-128
192	AES-192
256	AES-256

Size of Public Keys		
DSA/DH	**RSA**	**ECC**
1024	1024	160
2048	2048	224
3072	3072	256
7680	7680	384
15360	15360	512