An introduction of Cryptology

Pusan National University Computer Security Group

작성자 : 박상욱, 이현창

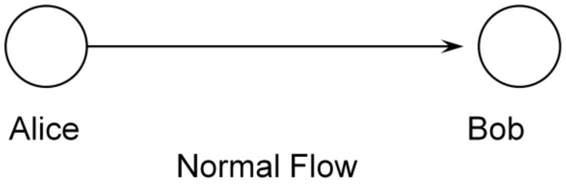
Contents --------------------

1. Introduction

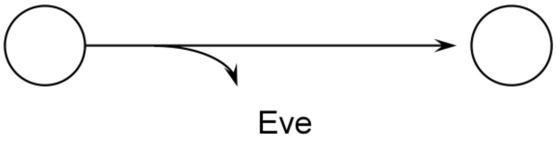
   -conception

   - ❑ Cryptography
     - ■ designing systems to do secure communication over insecure channels
   - ❑ Cryptanalysis
     - ■ breaking such systems

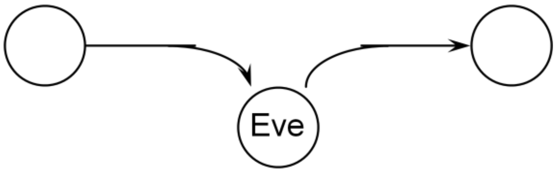
2. threat method



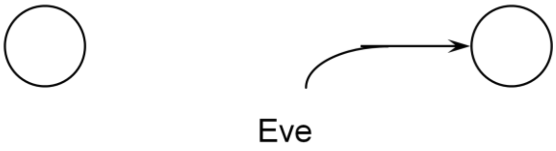
-1.Eavesdropping (prevent by confidentiality)



-2.Modification (prevent by Integrity)



-3.Impersonation (prevent by Authentication)



3. Security Services.
   1. Confidentiality – any person cannot read the middle of transmission

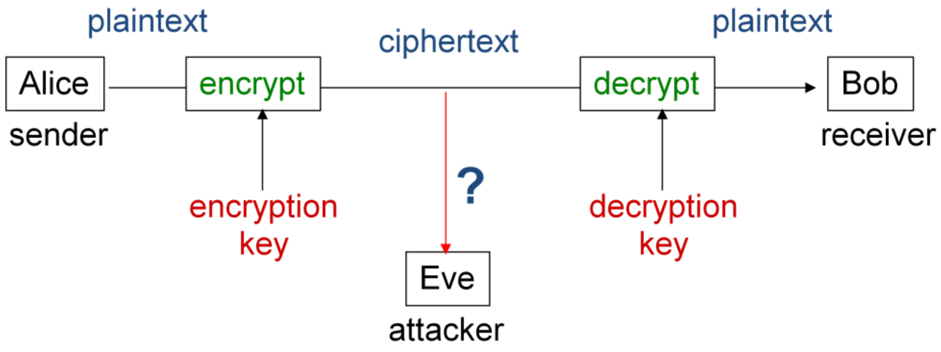
      (Encryption algorithm – Symmetric key algorithms, public key algorithms, etc.)
   2. Integrity – Receiver check that transmitter's sending data has not been changed.

      (Digital Signature – RSA, DSA)
   3. Authentication – Receiver make sure that communication partner is correct transmitter

   4. Access Control – Prevention of unauthorized use of a resource

   5. Availability – A system or a system resource should be accessible and usable

4. Confidentiality Model



5. Classical Cryptosystems

A. Shift Ciphers

Encryption method

Eliminate all spaces -> Shift each letter by (N) places

Decryption method

Shift back by (N)spaces

Attack method

Substitution all the 26 ways, known plaintext attack

B. Monoalphabetic Substitution Ciphers

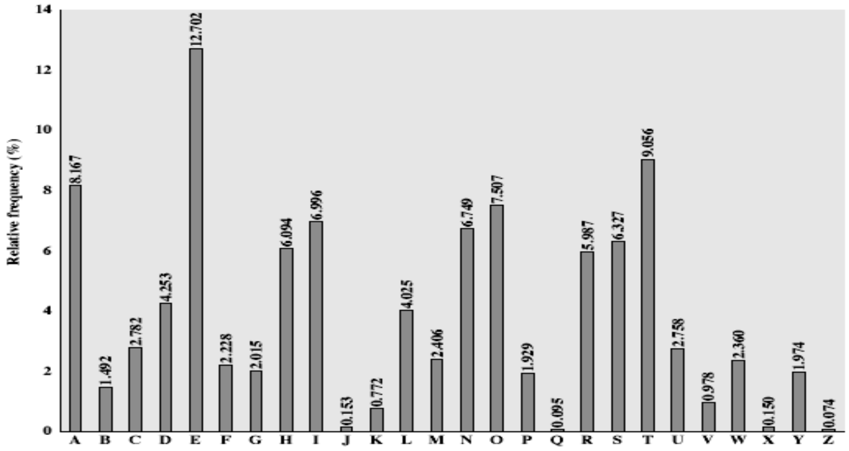
Encryption method

Eliminate all spaces -> Substitute 26 alphabets by other alphabets without rules

Attack method

Based on English sentence :

alphabet 'e' is the most included. The second is 't', the third is 'a'.



C. Transposition Ciphers

Encryption method

There are many methods. Rail Fence Cipher, Row Transposition Ciphers are representative

Row Transposition ciphers example.

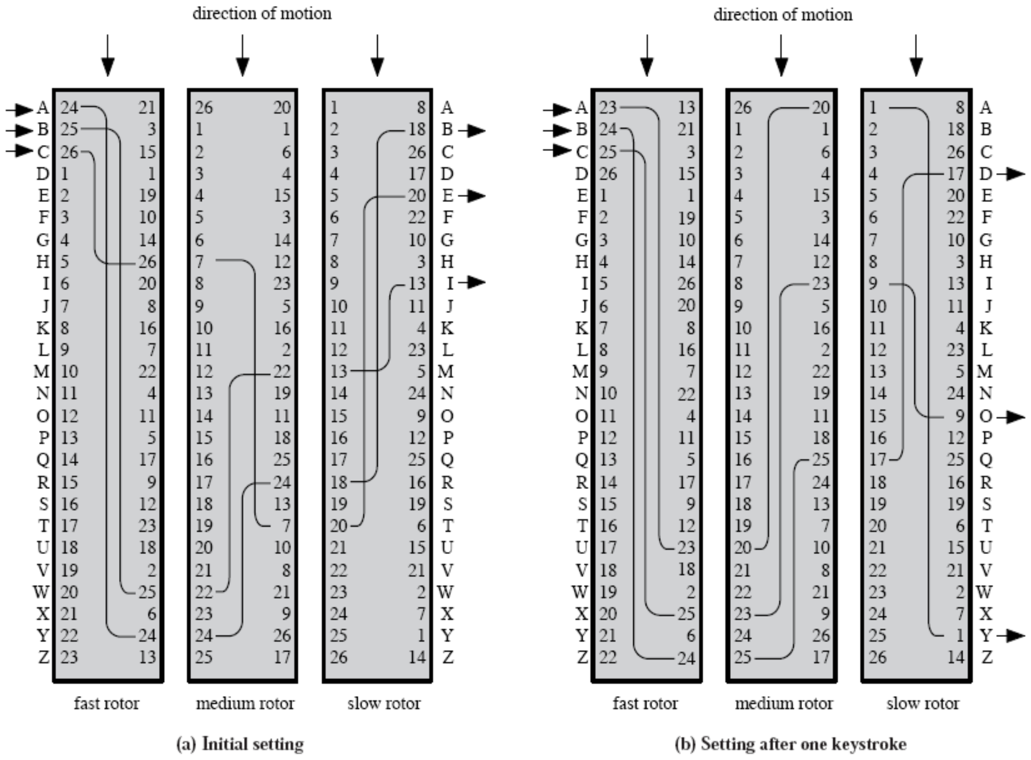
1. write letters of message out in rows over a specified number of columns.
2. Reorder the columns according to some key before reading off the rows

Key	4	3	1	2	5	6	7
Plaintext	a	t	t	a	c	k	P
	o	s	t	p	o	n	e
	d	u	n	t	i	l	T
	w	o	a	m	x	y	z
Ciphertext	TTNAAPTMTSUOAODWCOIXKNLYPETZ						

D. Rotor Machines.

Before modern ciphers, rotor machines were most common product cipher. Rotor Machines were widely used in World War II. Used a series of cylinders, each giving one substitution, which rotated and changed after each letter was encrypted

German – Enigma, Allied – Hagelin, Japanese – Purple



(a) Initial setting

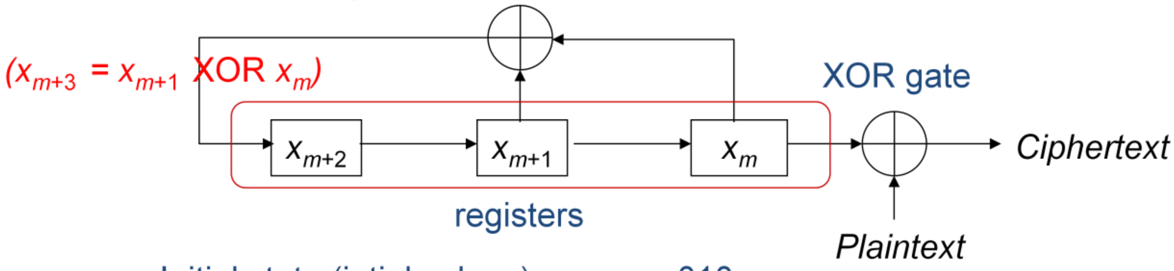
(b) Setting after one keystroke

Three-Rotor Machine With Wiring Represented by Numbered Contacts

6. LFSR Sequences.

   LFSR means Linear Feedback Shift Register. It's defined by a linear recurrence. LFSR implemented very easily, especially in hardware. And fast encode speed is advantage point too.

Example: $x_{m+3} = x_{m+1}$ XOR x_m



Initial state (intial values): $x_1x_2x_3$ = 010

Generated sequence: 0101110010111001…

Plaintext (AB…): 0100000101000010…

Ciphertext: 0001110111111011…

m=1 : $x_4=x_2$ xor x_1 = 1 xor 0 = 1
m=2: $x_5=x_3$ xor x_2 = 0 xor 1 = 1
m=3: $x_6=x_4$ xor x_3 = 1 xor 0 = 1
m=4: $x_7=x_5$ xor x_4 = 1 xor 1 = 0
m=5: $x_8=x_6$ xor x_5 = 1 xor 1 = 0
m=6: $x_9=x_7$ xor x_6 = 0 xor 1 = 1

m=7 : $x_{10}=x_8$ xor x_7 = 0 xor 0 = 0
m=8 : $x_{11}=x_9$ xor x_8 = 1 xor 0 = 1
m=9 : $x_{12}=x_{10}$ xor x_9 = 0 xor 1 = 1
m=10: $x_{13}=x_{11}$ xor x_{10} = 1 xor 0 = 1
m=11: $x_{14}=x_{12}$ xor x_{11} = 1 xor 1 = 0
m=12: $x_{15}=x_{13}$ xor x_{12} = 1 xor 1 = 0

Unfortunately, this encryption method succumbs easily to a known plaintext attack. This is because the construction is linear. If we know only a few consecutive bits of plaintext, along with the corresponding bits of ciphertext, an attack can determine the whole sequence. It is known that an attacker can recover the linear recurrence if (2n) consecutive elements in the sequence is revealed.

->Improvement : The problem is that the recurrence is linear, and an attacker can make matrix equation. So, we append some nonlinear elements.

7. DES(Data Encryption Standard)

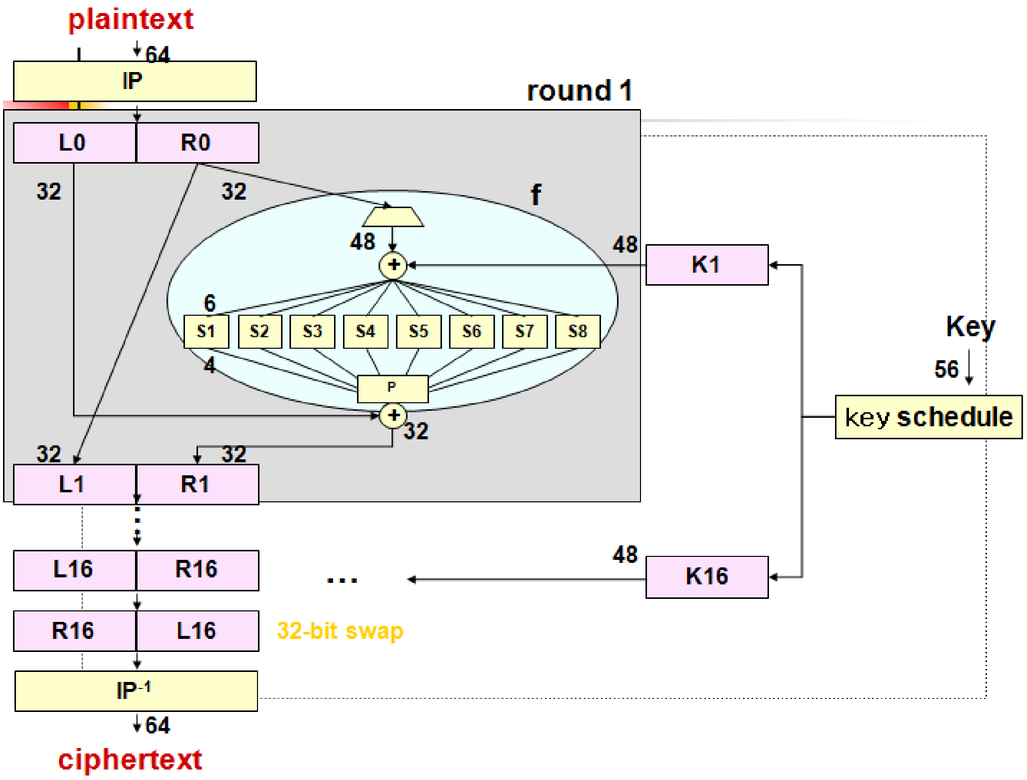
   A. History .

      DES is most widely used block cipher in world. It adopted in 1977 by NBS(now NIST). It encrypts 64bit data using 56bit key. It has been considerable controversy over its security.

      IBM(by team led by Feistel) developed Lucifer cipher. It used 64bit data blocks with 128bit key. Then redeveloped as a commericial cipher with input from NSA and others. In 1973 NBS issued request for proposals for a national cipher standard. IBM submitted their revised Lucifer which was eventually accepted as the DES

DES has became widely used, especially in financial applications until 1998. In 1998 Electronic Frontier Foundation (EFF) implemented indiscriminate substitute attack. And it broke DES in 56hours. Nowadays, AES(Advanced Encryption Standard) is frequently used.

B. Algorithm



1. Input 64bit plaintext and apply IP rule(referencing IP table)
2. Separate 64bit by 32bit and expansion right side of 32bit to 48bit(referencing Expansion Permutation E table)
3. Do XOR with expanded 48bit and 48bit Key(K1)
4. Divide 8 parts like picture and apply each S(n) rule. And each 6bit parts downsized by 4bit parts. And assemble them.
5. Do XOR with left side of 32bit and assembled 32bit.
6. Process 5 is method of making R1. And right side of 32bit is turn over to L1.
7. Process 1~6 is apply to Round 1. And repeat the process to 16 times.(every time, key data changed.)
8. Decryption is same as encryption. We can use the same structure, but with

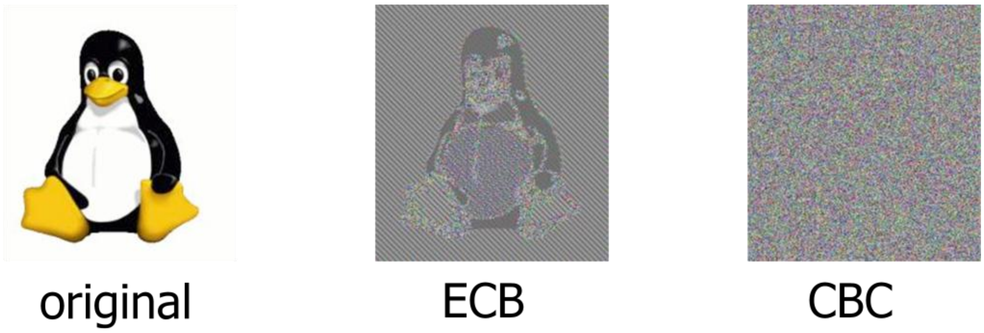
the subkeys used in reverse table order.

Caution : in the midst of 64bit keys, only 56 bit are real keys. 8 bit are parity-check bits for error detect

8. ECB(Electronic Codebook Book)

   Message is broken into independent blocks which are encrypted. Each block is a value which is substituted, like a codebook.

   But limitations of ECB is existed. Repetitions in message may show in ciphertext



original ECB CBC

9. CBC(Cipher Block Chaining)

   CBC make message broken into blocks, and these are linked together in the encryption operation. Each previous cipher blocks is chained with current plaintext block. CBC use Initial Vetor(IV) to start process. So, CBC has limitation that each ciphertext block depends on all message blocks, thus a change in the message affects all ciphertext blocks after the change as well as the original block.

10. AES(Advanced Encryption Standard)

    National Institute of Standards and Technology(NIST) set this AES to world benchmark. At 2002. It was called “Rijndael” that original publisher. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The blocksize has a maximum of 256 bits, but the keysize has theoretically no maximum.

    The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use."

A. Algorithm

1. Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule

2. Initial Round
   a. AddRoundKey - each byte of the state is combined with the round key using bitwise xor

3. Rounds
   a. SubBytes - each byte is replaced with another according to a lookup table. This operation provides the non-linearity in the cipher.
   b. ShiftRows – each row of the state is rotate by a certain number of steps
   c. MixColumns - the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher.
   d. AddRoundkKey – In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

4. Final Round(no MixColumns)
   a. SubBytes
   b. ShiftRows
   c. AddRoundKey

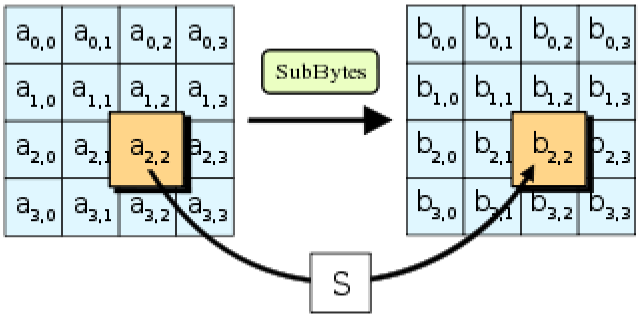

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

그림 1 In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; bij = S(aij).

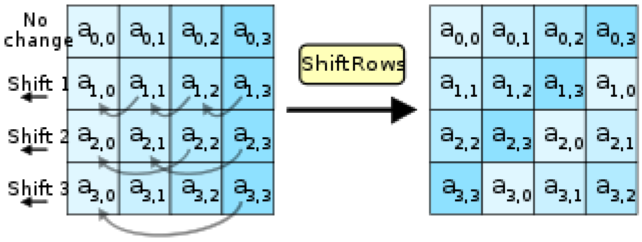


그림 2 In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

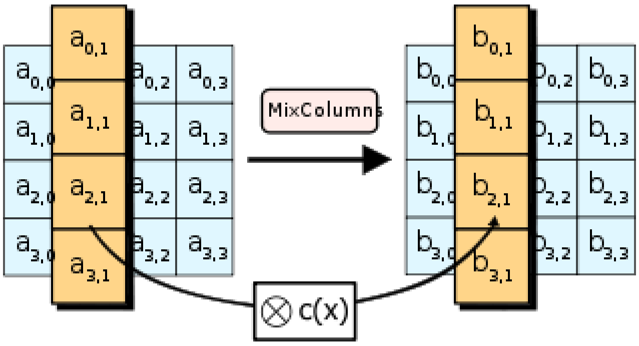


그림 3 In the MixColumns step, each column of the state is multiplied with a fixed polynomial c(x).

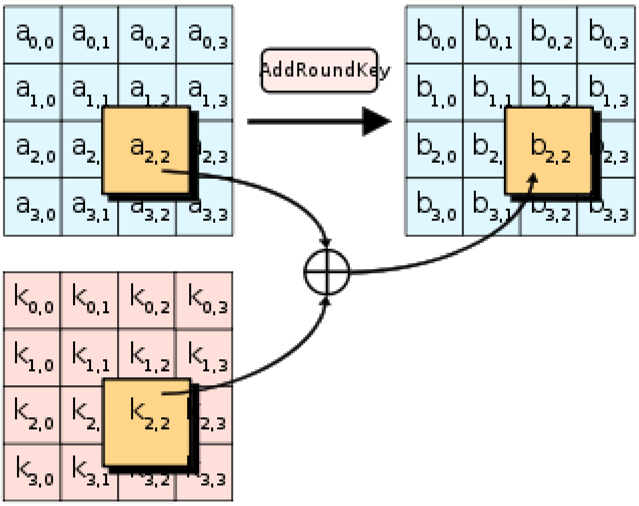


그림 4 In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

B. Attack method : XSL attacking

The XSL attacking is method of breaking block ciphers. This attack was first published in 2002 by researchers Nicolas Courtois and Josef Pieprzyk. Since AES is already widely used in commerce and government for the transmission of secret information, finding a technique that can shorten the amount of time it takes to retrieve the secret message without having the key could have wide impacts.

11. Reference

http://en.wikipedia.org/wiki/XSL_attack#Application_to_block_ciphers
http://en.wikipedia.org/wiki/Rijndael
http://blog.naver.com/proonan29?Redirect=Log&logNo=130082479064
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Professor Ho – Won Kim's
Computer Security Class - 1_Introduction_to_Cryptography_and_Security.ppt
Computer Security Class - 2_Introduction_to_Cryptography_and_Security.ppt
Computer Security Class - 3_Block_Ciphers_and_DES