

Block Ciphers and DES

Harshan Jagadeesh
Department of Electrical Engineering,
IIT Delhi

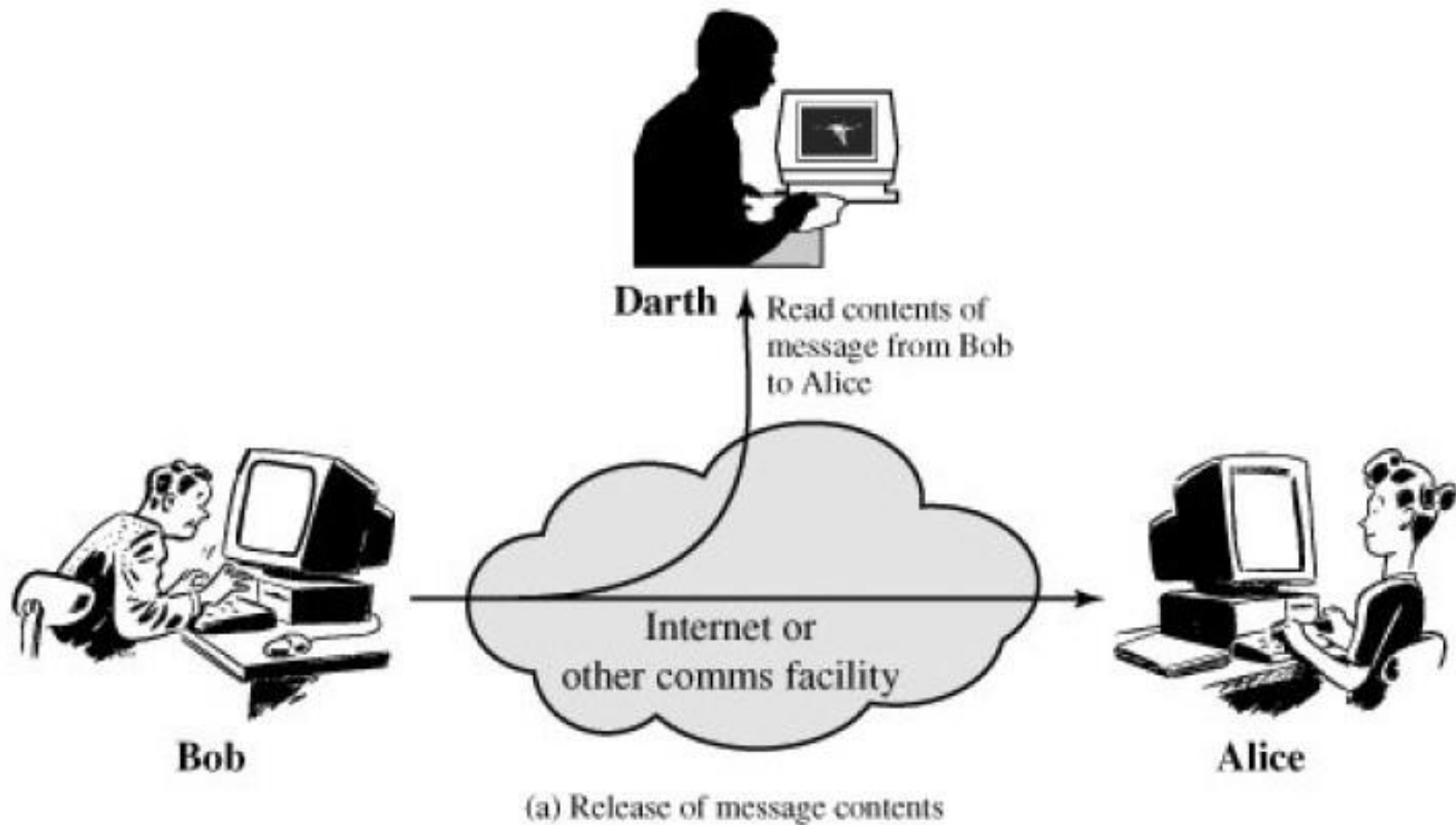


References and notes used from:

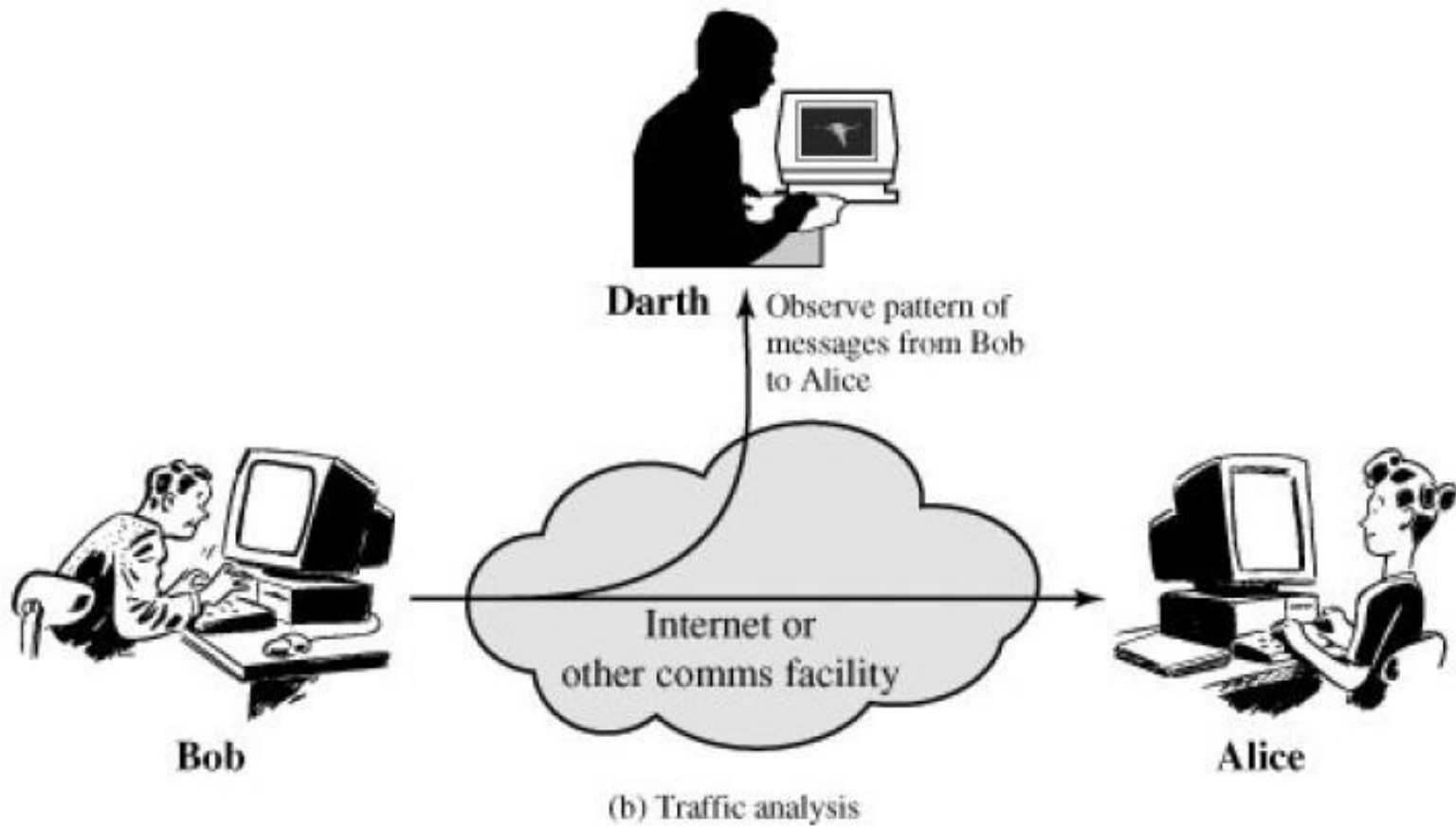
Cryptography and Network Security, Principles and Practices, by William Stallings
(combination of several editions)

Cryptography and network security course at SCSE, NTU by Prof. Anwitaman Datta

Motivation - Confidentiality



Motivation - Confidentiality



A Unifying Solution – So Far!

Use of shared secret keys at the legitimate entities

Construct problems

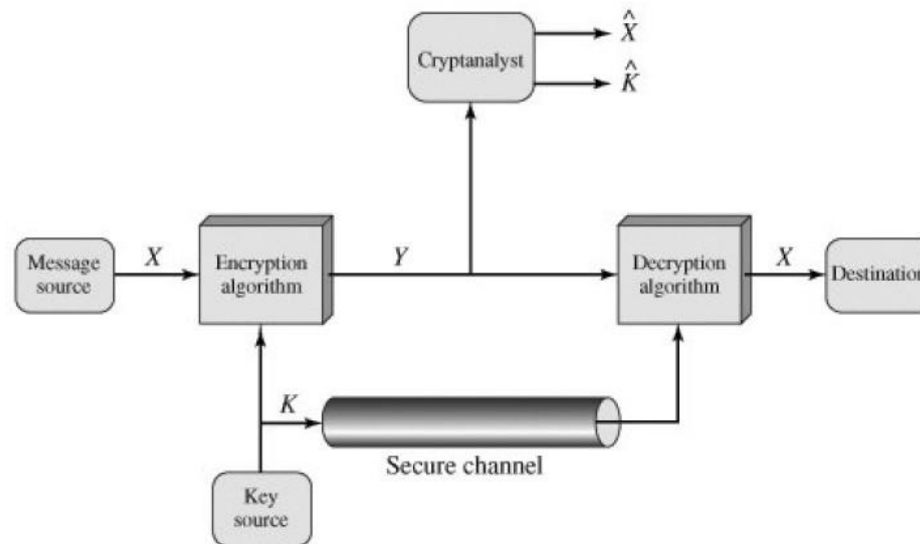
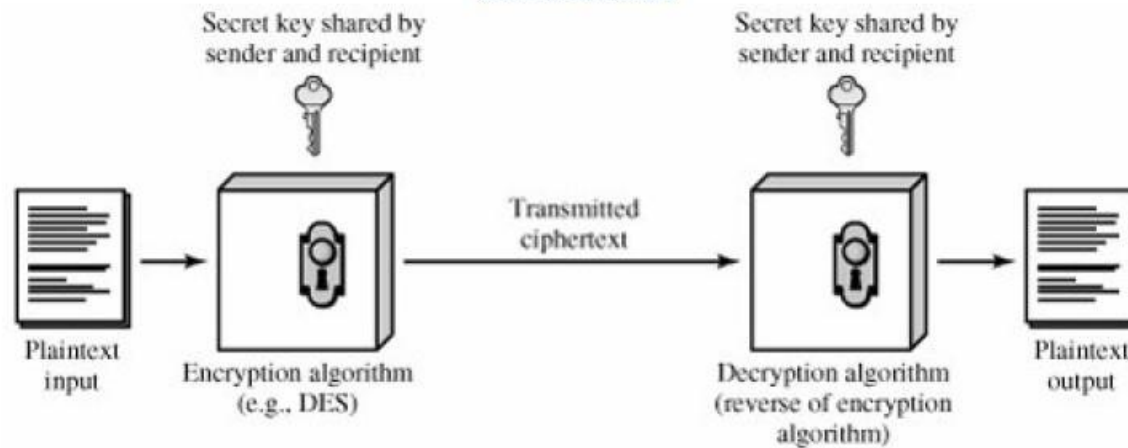
1. Easy to solve with key
2. Hard to solve without key

Bounded computational complexity at the adversary



*google images

Symmetric Key Encryption



Principles of Symmetric Key Cryptography

1. Substitution

1. Substitute plaintext symbols
2. Monoalphabetic substitution is vulnerable to frequency analysis
3. Polyalphabetic substitution is resilient – beyond a point not easy to implement

2. Transposition

1. Reorder the sequence of symbols in the plaintext (permutation)

3. Cascade

1. Have a simple structure as kernel (for ease of implementation) and then cascade them for stronger security

Transposition – Some Ideas

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

Apply again:

Key:	4	3	1	2	5	6	7
Input:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Steganography

3rd March

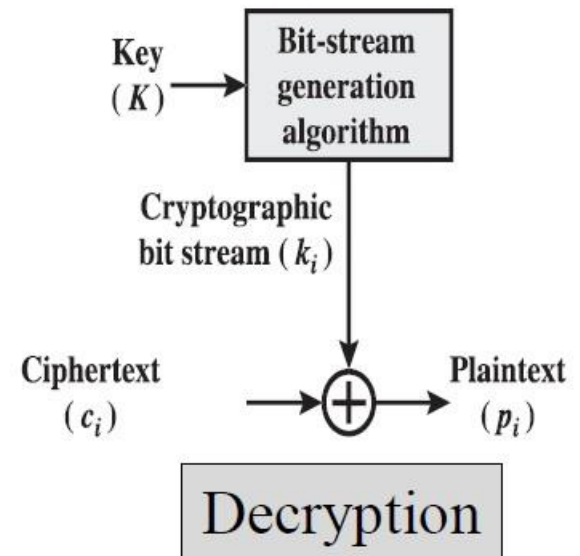
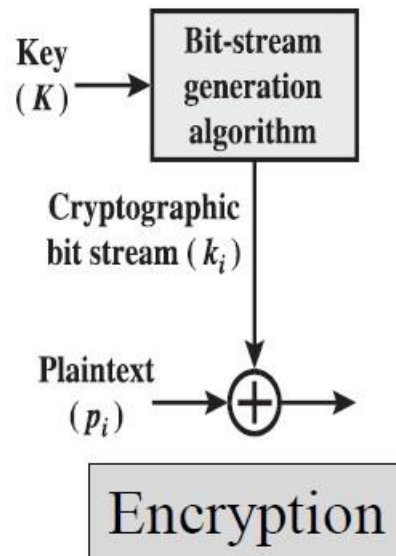
Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16t proposals destroy your basis O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

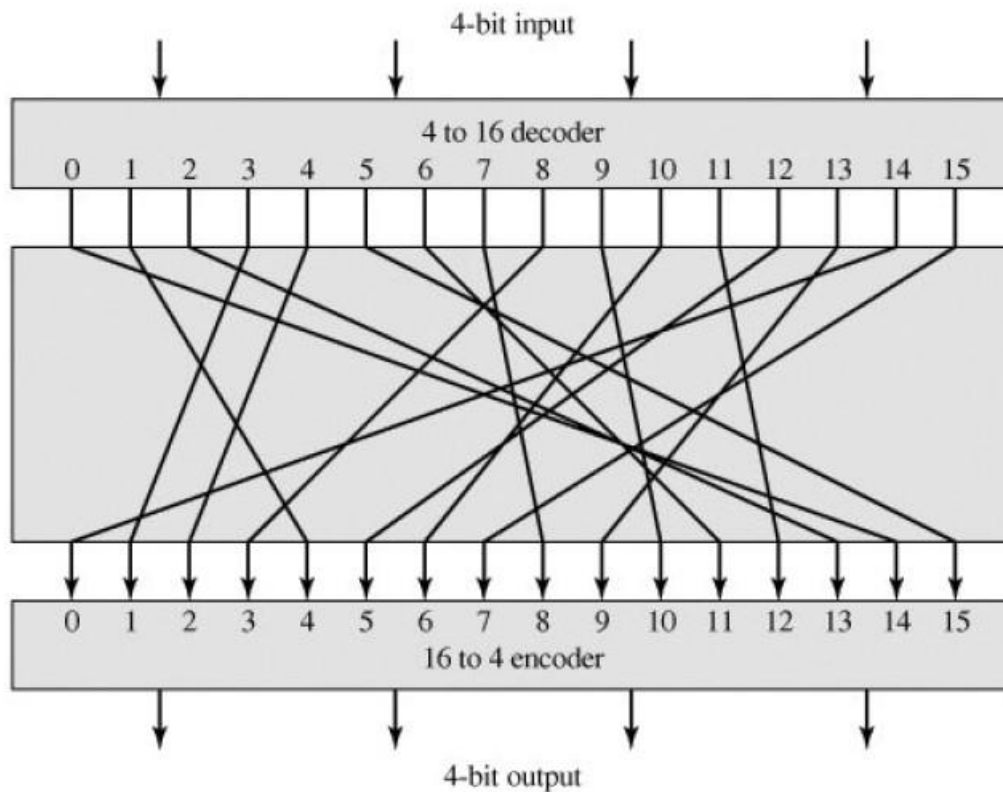
Sincerely yours.

Stream Ciphers

1. One symbol at a time
2. Monoalphabetic substitution
3. One time pad as an example
4. How to realize this in practice?



Block Ciphers



Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Represent this mapping using 4×16 bits

In general, represent this mapping using $n \times 2^n$ bits secret key

Block Ciphers

Design principles

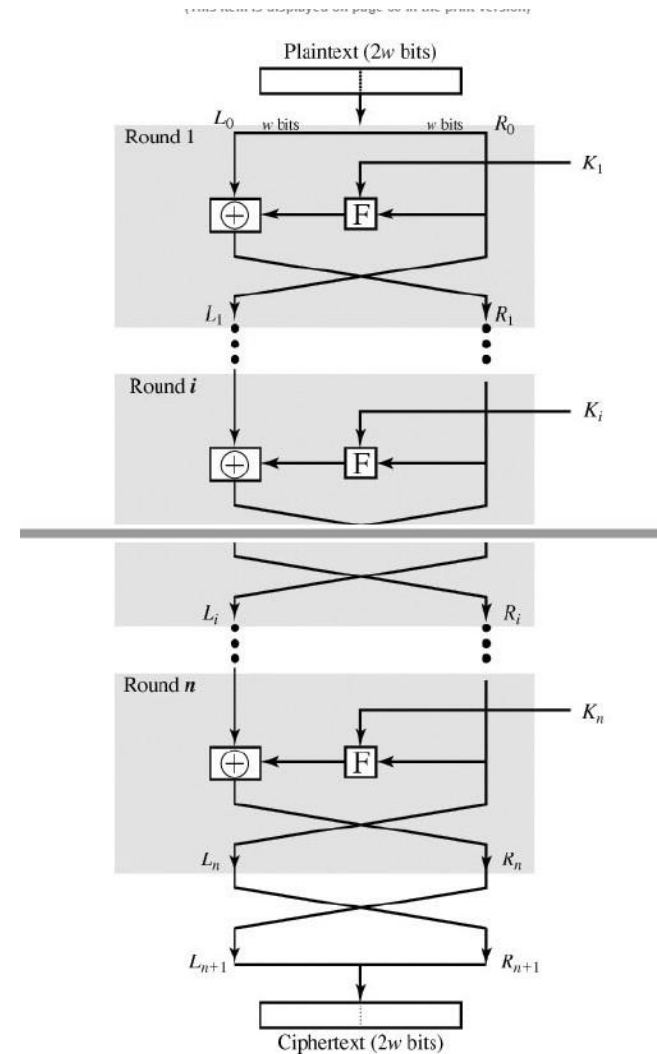
1. Diffusion – dissipate the statistical structure of the plaintext across the ciphertext
 2. Confusion – make the relation between the statistics of ciphertext and key as complex as possible
 3. Cascade – easy implementation and yet strongly secure
-
1. Follow the substitution-permutation framework
 2. Feistel proposed a network using a combination of substitution and permutation

Feistel Cipher

1. Repeat substitution block for multiple rounds
2. Apply permutation by dividing the plaintext into two halves
3. Use multiple short keys for ease of implementation

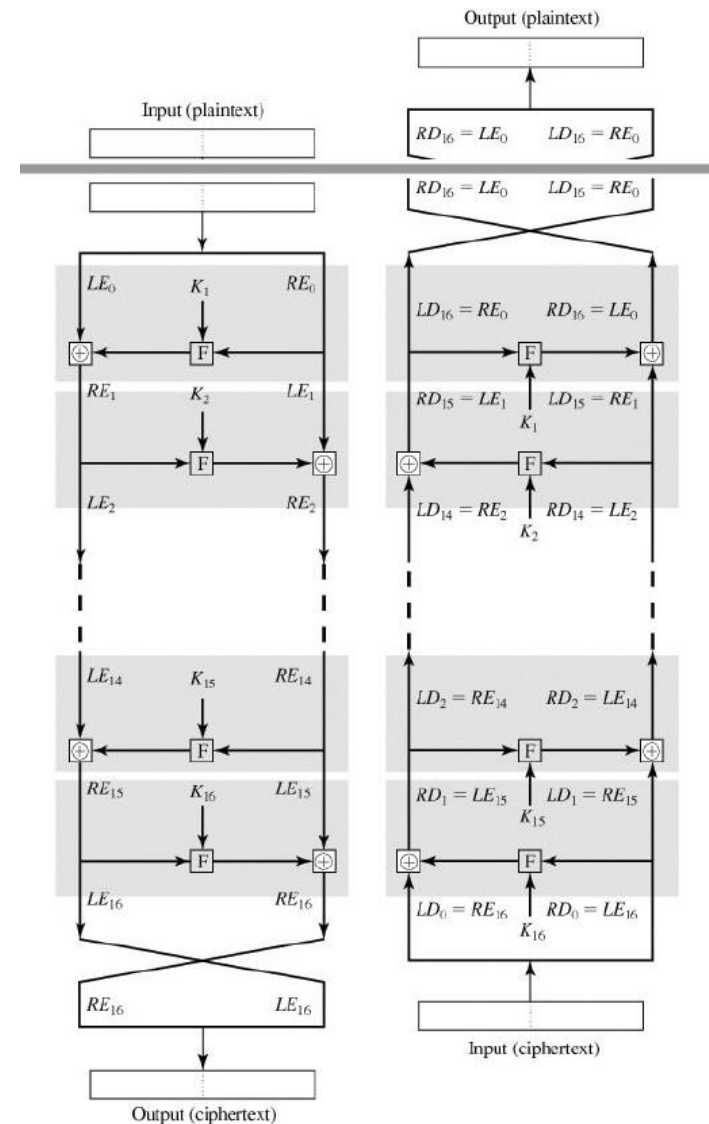


Horst Feistel
1915-1990



Feistel Cipher

1. No need to perform inverse of rounding function
2. Repeat the same process in the reverse direction



Data Encryption Standard

LUCIFER: Lloyd's
London cash
dispensing machine

1971

Adopted as
Data Encryption
Standard (**DES**)

1977

Electronic Frontier Foundation
(**EFF**) breaks DES w/ \$250K
machine

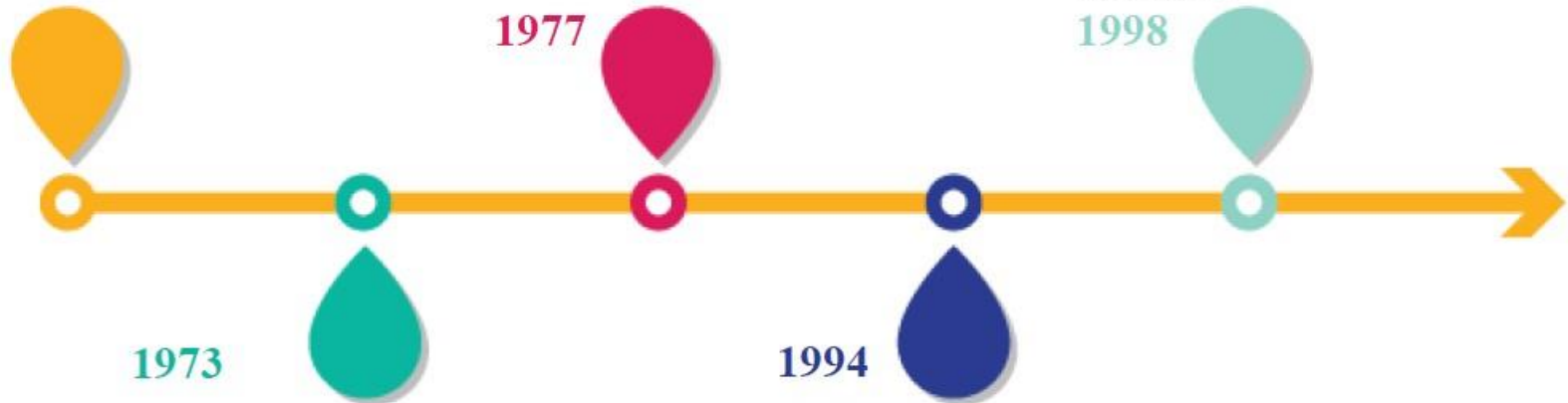
1998

1973

National Bureau for
Standards (**NBS**) RFP for
national cipher standard

1994

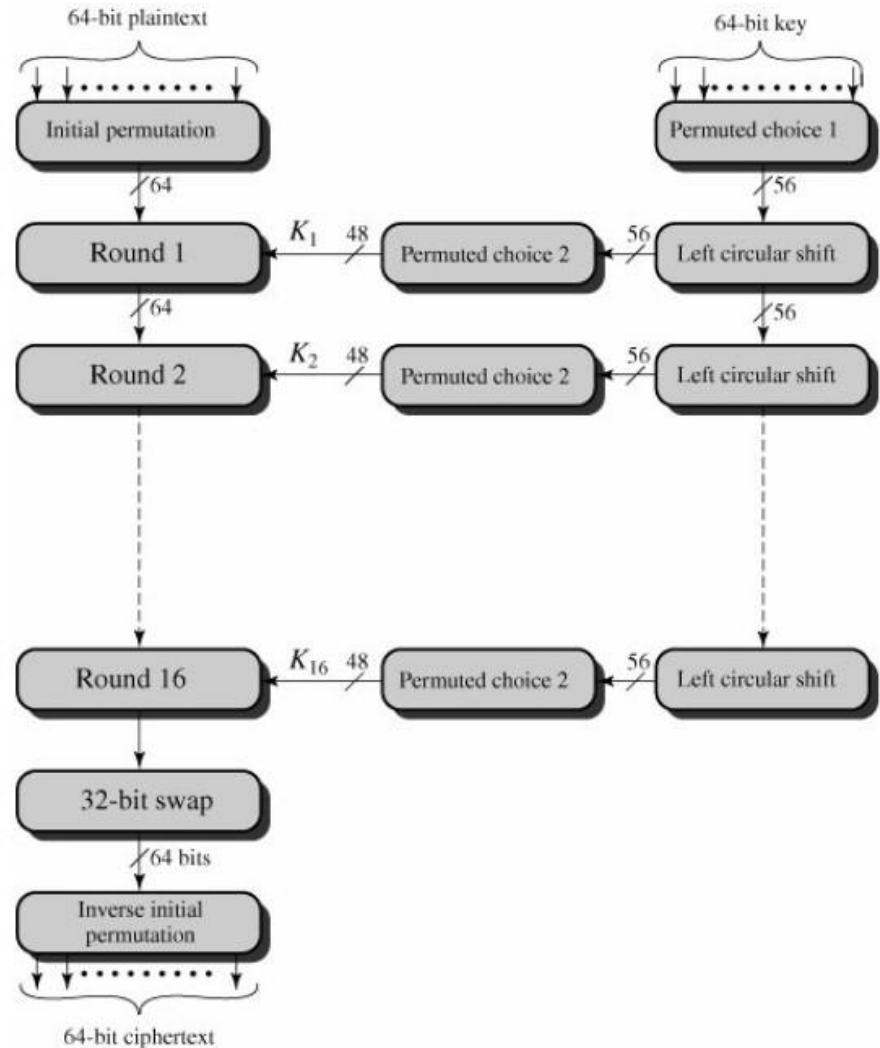
National Institute of
Standards and Technology
(**NIST**) reaffirms DES for
federal use



Data Encryption Standard

This follows the principles
of Feistel network

Although the secret-key is 64 bits,
Only 56 bits are used



DES

Permutation block of plaintext

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

Inverse of permutation

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

DES

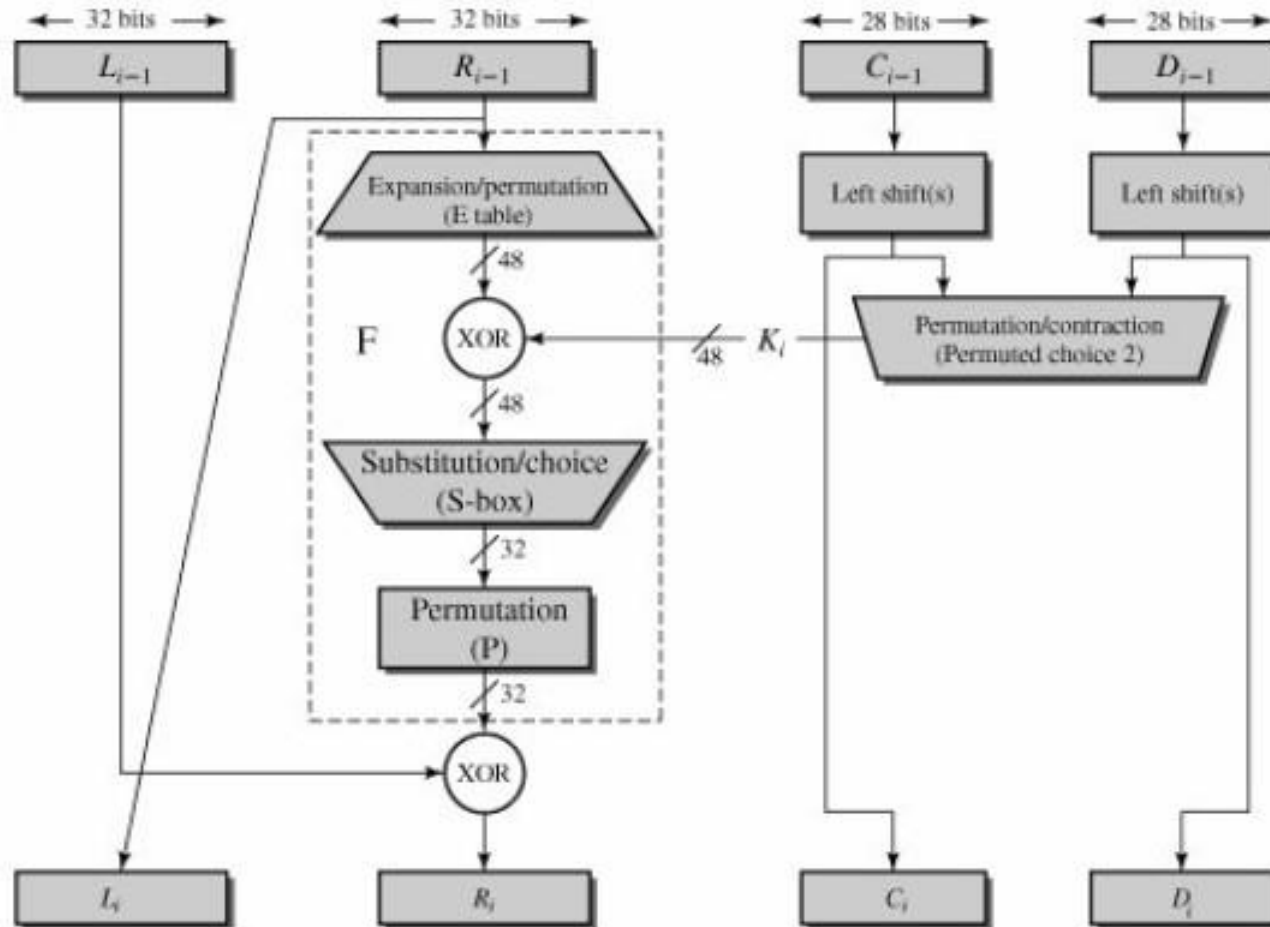
Write the plaintext as below

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

Read them as below

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

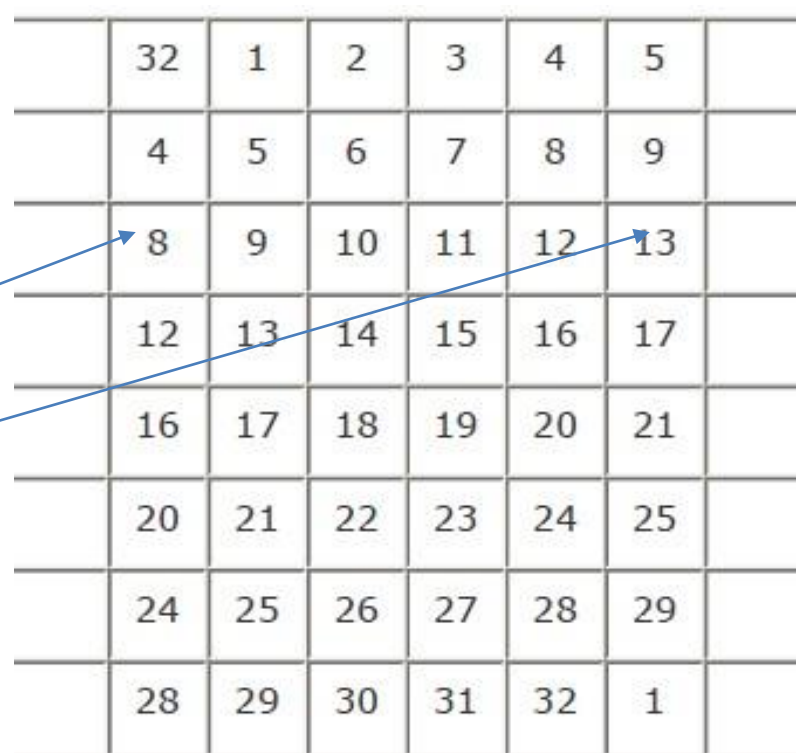
DES – What happens every round?



DES

Expansion block: 23 bits to 48 bits (redundancy addition)

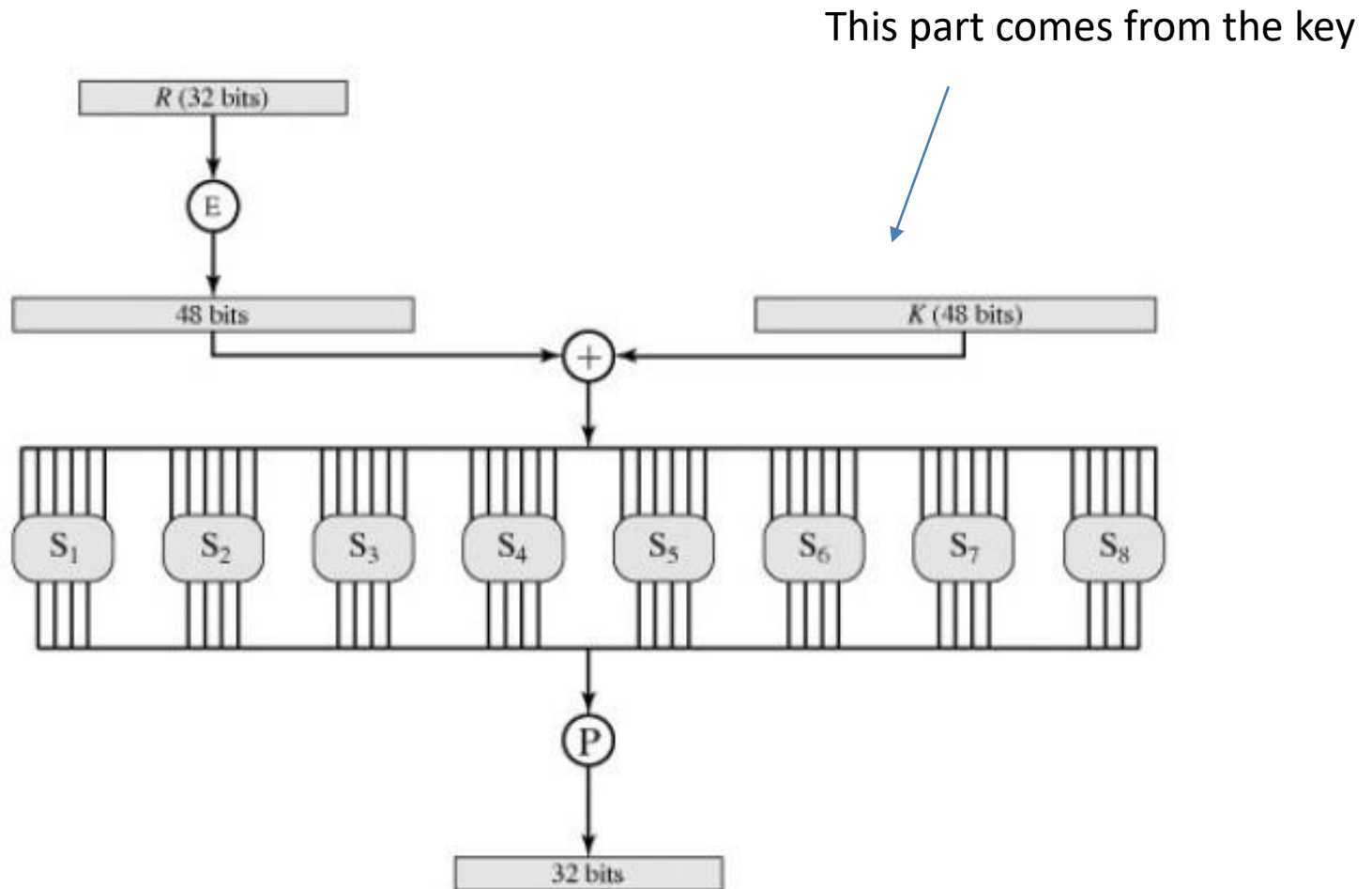
Additional columns inserted



	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	

DES

Substitution block



DES

Substitution block mapping

1. Which row to choose is given by the first and the last bit
2. Use the appropriate column from the middle bits

$$S_1$$

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

$$S_2$$

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

$$S_3$$

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

$$S_4$$

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

$$S_5$$

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

$$S_6$$

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

$$S_7$$

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

$$S_8$$

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

DES

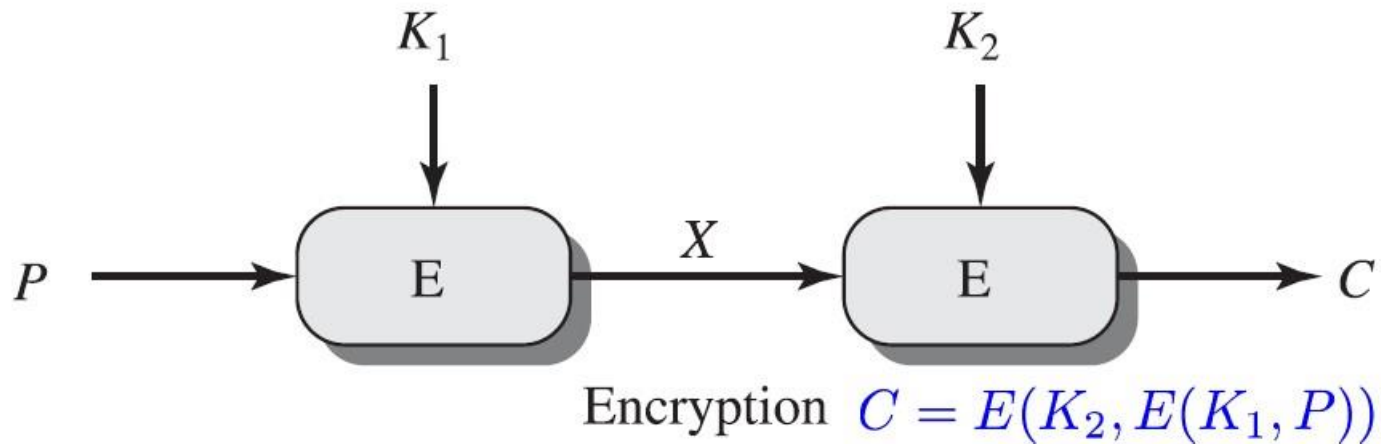
One more round of permutation after substitution

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

What to do with a broken cipher?

In 1998, Electronic Frontier Foundation breaks by using a \$250K machine

Not a problem!! Apply DES twice



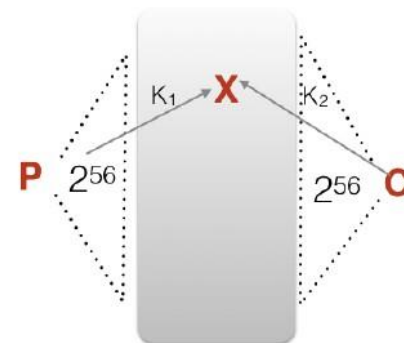
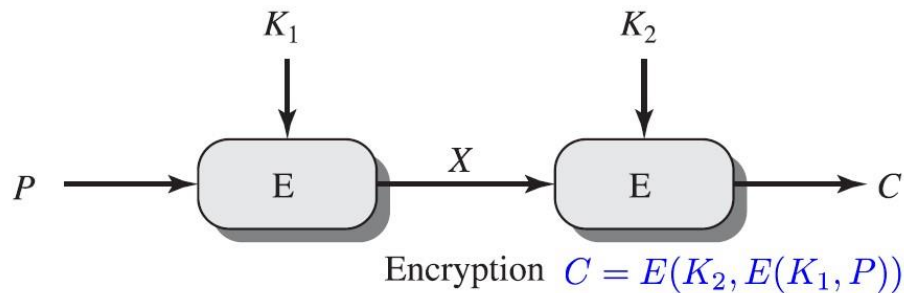
What to do with a broken cipher?

What if

1. Cascaded block cipher is equivalent to one cipher?

What if: $E(K_2, E(K_1, P)) \equiv E(K_3, P)$

2. Meet-in-the-middle attack – Use known plain text and also break the second DES



What to do with a broken cipher?

1. Encrypt three times!! – This is called Triple DES
2. Meet-in-the-middle attack – very low threat probability
3. Use two keys for three rounds – that's good enough

$$C = E(K_1, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_1, P)))$$

What's the problem of triple DES?

1. Computation efficiency is a problem
2. NIST released a call for proposal for Advanced Encryption Standard after the DES development
3. Roughly 15 proposals were received
4. After shortlist and review, Rijndael was accepted.
5. Introduced to standards in 2001



Vincent Rijmen
born in 1970



Joan Daemen
born in 1965