

ECE 646 - Lecture 7

Data Encryption Standard RC5

1

Levels of Security

Definition: Unconditional Security

A cryptosystem is unconditionally secure if it cannot be broken even with infinite computational resources.

Q: Which actual cryptosystems are unconditionally secure?

3

Levels of Security

Definition: Computational Security

A cryptosystem is “computational secure” if **best possible algorithm** for breaking requires N operations, where N is very large and known.

Q: Which actual cryptosystems are “computational secure”?

4

Levels of Security

Definition: Relative Security

A cryptosystem is “relative secure” if its security relies on a well studied, very hard problem.

Q: Which actual cryptosystems are “relative secure”?

5

Data Encryption Standard

6

NBS public request for a standard cryptographic algorithm
May 15, 1973, August 27, 1974

The algorithm must be:

- secure
- public
 - completely specified
 - easy to understand
 - available to all users
- economic and efficient in hardware
- able to be validated
- exportable

7

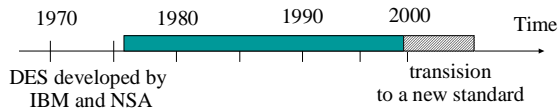
DES - chronicle of events

- 1973 - NBS issues a public request for proposals for a standard cryptographic algorithm**
- 1975 - first publication of the IBM's algorithm and request for comments**
- 1976 - NBS organizes two workshops to evaluate the algorithm**
- 1977 - official publication as FIPS PUB 46: Data Encryption Standard**
- 1983, 1987, 1993 - recertification of the algorithm for another five years**
- 1993 - software implementations allowed to be validated**

Controversies surrounding DES

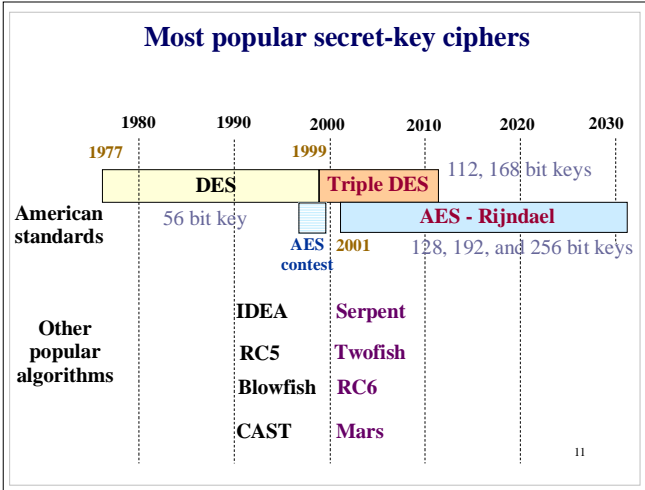
Unknown design criteria	Slow in software	Key too short
Most criteria reconstructed from cipher analysis 1990 Reinvention of differential cryptanalysis	Only hardware implementations certified 1993 Software, firmware and hardware treated equally	Theoretical designs of DES breaking machines 1998 Practical DES cracker built

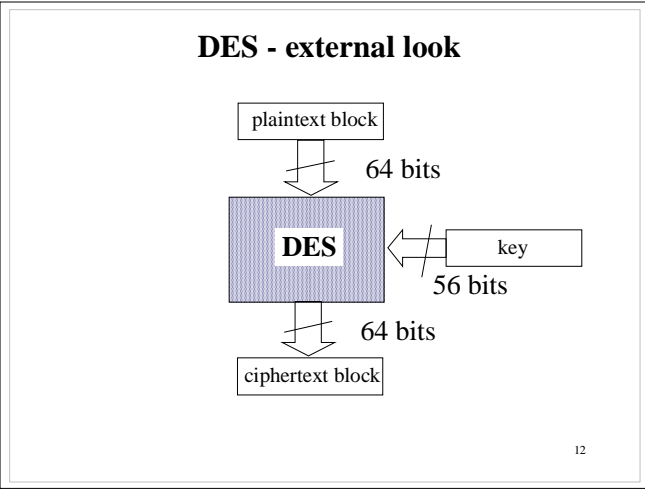
Life of DES

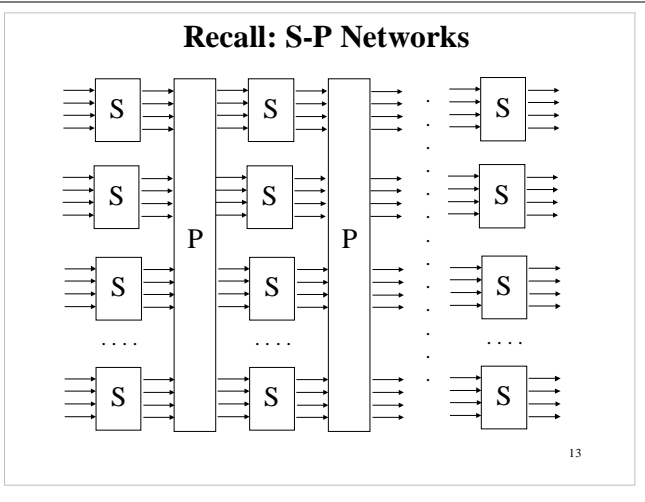


In common use for over 20 years

- Federal and banking standard
- Over 300 validated implementations
- De facto world-wide standard





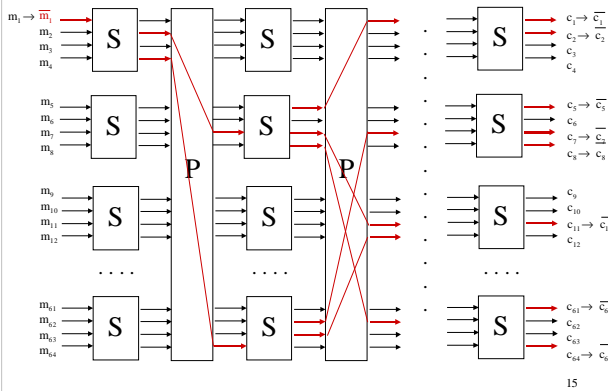


Confusion / Diffusion

- **Confusion**
 - relationship between cleartext and ciphertext is obscured
 - e.g. substitution (Shift Cipher, Enigma)
- **Diffusion**
 - spreading influence of one cleartext letter to many ciphertext letters
 - e.g. permutations

14

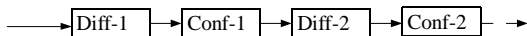
Recall: Avalanche effect



15

Iterated Product Cipher

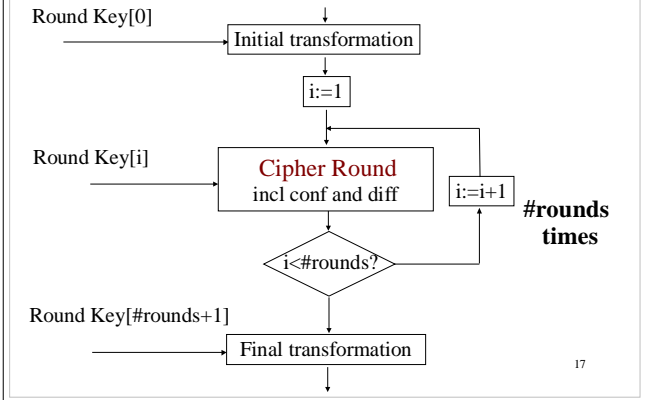
- Combine confusion with diffusion
- Multiple “Rounds” of confusion and diffusion



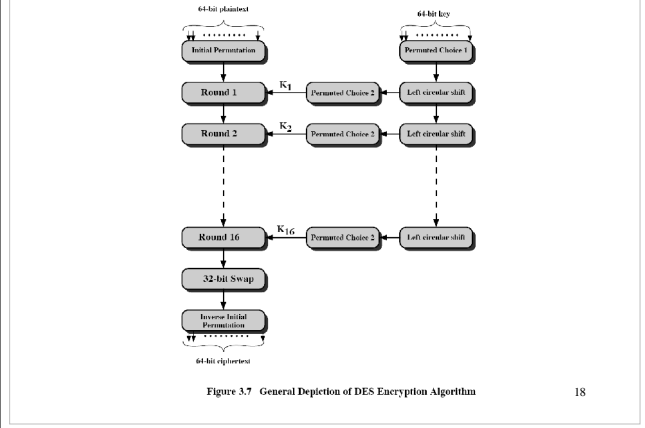
- Option to iterate over the same round or unroll all rounds

16

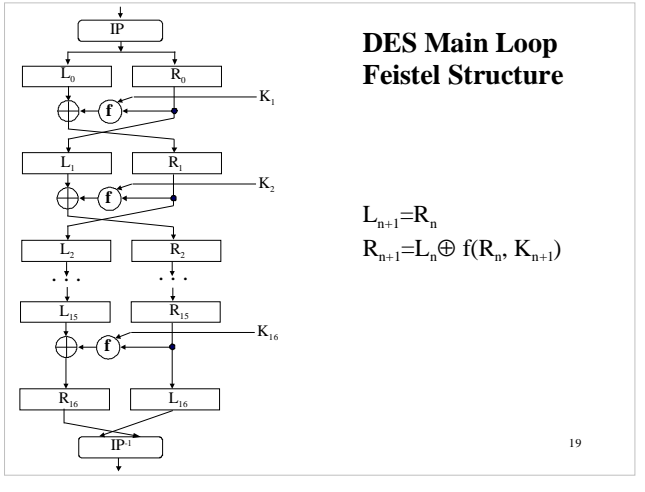
Typical Flow Diagram of a Secret-Key Block Cipher



DES – high-level internal structure

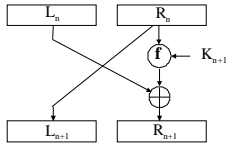


DES Main Loop Feistel Structure

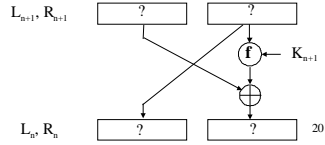
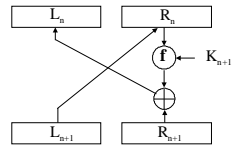


Feistel Structure

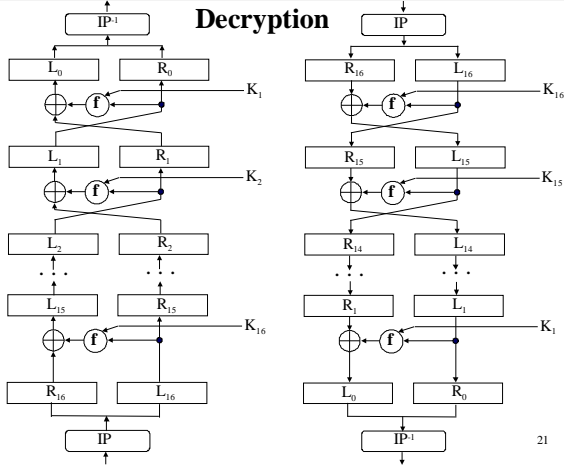
Encryption



Decryption



Decryption



21

Mangler Function of DES, F

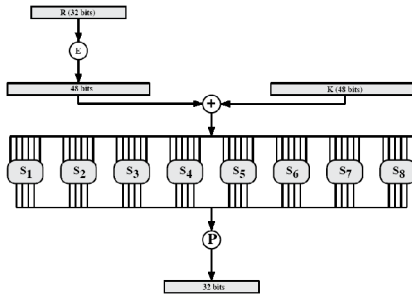


Figure 3.9 Calculation of $F(R, K)$

2

(a) Initial Permutation (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

(b) Inverse Initial Permutation (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

(c) Expansion Permutation (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

(d) Permutation Function (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

23

Notation for Permutations

Input

$$i_1 i_2 i_3 i_4 i_5 i_6 i_7 i_8 i_9 i_{10} \dots i_{56} i_{57} i_{58} i_{59} i_{60} i_{61} i_{62} i_{63} i_{64}$$

58 50 42 34 26 18 10 2 ... 5 63 55 47 39 31 23 15 7

$$i_{58} i_{50} i_{42} i_{34} i_{26} i_{18} i_{10} i_2 \dots i_5 i_{63} i_{55} i_{47} i_{39} i_{31} i_{23} i_{15} i_7$$

Output

24

Table A.2 Definition of DES S-boxes

S ₁	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S ₂	9	15	7	4	14	2	17	1	16	6	12	11	8	3	10	5
S ₃	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
S ₄	15	12	8	2	4	9	1	7	5	11	3	14	10	6	9	13
S ₅	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
S ₆	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
S ₇	8	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
S ₈	13	8	16	1	3	15	4	5	13	6	7	12	0	3	14	9
S ₉	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
S ₁₀	15	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
S ₁₁	12	6	4	9	8	15	3	0	13	11	2	12	5	10	14	7
S ₁₂	1	10	15	0	6	9	8	7	4	13	14	3	11	5	2	12
S ₁₃	7	12	14	3	0	6	9	10	1	2	8	5	11	12	4	15
S ₁₄	13	8	15	5	6	15	0	3	4	7	12	1	10	14	9	2
S ₁₅	10	6	9	0	12	14	7	13	10	1	3	14	5	2	8	11
S ₁₆	3	15	6	6	10	1	12	8	9	4	5	11	12	7	2	14
S ₁₇	2	12	4	1	7	10	11	0	9	5	3	15	13	5	14	9
S ₁₈	14	11	2	12	4	7	13	1	3	0	15	10	1	9	8	6
S ₁₉	4	2	1	11	10	13	7	3	15	9	12	5	6	3	0	14
S ₂₀	11	8	12	7	1	14	2	13	6	15	9	10	4	5	3	2
S ₂₁	13	1	10	15	9	2	6	3	0	15	3	4	14	7	5	11
S ₂₂	10	15	14	2	7	12	9	5	6	1	13	14	0	11	3	8
S ₂₃	9	14	15	1	7	8	12	3	7	0	4	10	1	15	11	6
S ₂₄	4	5	2	12	9	5	15	10	13	15	1	7	6	0	8	13
S ₂₅	4	11	2	14	15	0	8	13	3	12	5	7	3	15	6	1
S ₂₆	15	0	11	7	4	9	1	10	11	3	12	2	15	15	6	0
S ₂₇	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	12
S ₂₈	6	11	13	8	1	4	10	7	9	1	0	15	14	2	3	12
S ₂₉	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
S ₃₀	11	10	8	10	3	3	14	13	5	8	11	0	14	9	2	1
S ₃₁	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
S ₃₂	2	1	14	7	4	10	8	13	15	12	9	0	3	5	0	11

25

General design criteria of DES

1. Randomness

2. Avalanche property

changing a single bit at the input changes on average half of the bits at the output

3. Completeness property

every output bit is a complex function of all input bits (and not just a subset of input bits)

4. Nonlinearity

encryption function is non-affine for any value of the key

5. Correlation immunity

output bits are statistically independent of any subset of input bits

29

Completeness property

Every output bit is a complex function of all input bits
(and not just a subset of input bits)

Formal requirement:

For all values of i and j, $i=1..64, j=1..64$
there exist inputs X_1 and X_2 , such that

$$\begin{matrix} X_1 & x_1 & x_2 & x_3 & \dots & x_{i-1} & 0 & x_{i+1} & \dots & x_{63} & x_{64} \\ X_2 & x_1 & x_2 & x_3 & \dots & x_{i-1} & 1 & x_{i+1} & \dots & x_{63} & x_{64} \end{matrix}$$

$$\begin{matrix} Y_1 = \text{DES}(X_1) & y_1 & y_2 & y_3 & \dots & y_{j-1} & y_j & y_{j+1} & \dots & y_{63} & y_{64} \\ Y_2 = \text{DES}(X_2) & y_1' & y_2' & y_3' & \dots & y_{j-1}' & \overline{y_j} & y_{j+1}' & \dots & y_{63}' & y_{64}' \end{matrix}$$

30

Linear Transformations

Transformations that fulfill the condition:

$$T(X_{[m \times 1]}) = Y_{[n \times 1]} = A_{[n \times m]} \cdot X_{[m \times 1]}$$

or

$$T(X_1 \oplus X_2) = T(X_1) \oplus T(X_2)$$

Affine Transformations

Transformations that fulfill the condition:

$$T(X_{[m \times 1]}) = Y_{[n \times 1]} = A_{[n \times m]} \cdot X_{[m \times 1]} \oplus B_{[n \times 1]}$$

31

Linear Transformations of DES

IP, IP⁻¹, E, PC1, PC2, SHIFT

e.g.,

$$IP(X_1 \oplus X_2) = IP(X_1) \oplus IP(X_2)$$

Non-Linear and non-affine transformations of DES

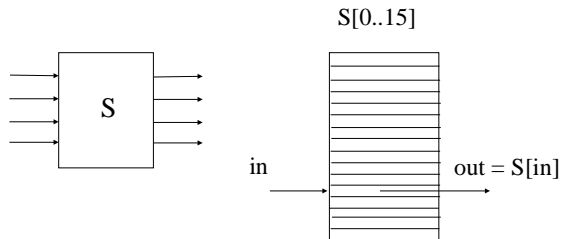
S

There are no such matrices $A_{[4 \times 6]}$ and $B_{[4 \times 1]}$ that

$$S(X_{[6 \times 1]}) = A_{[4 \times 6]} \cdot X_{[6 \times 1]} \oplus B_{[4 \times 1]}$$

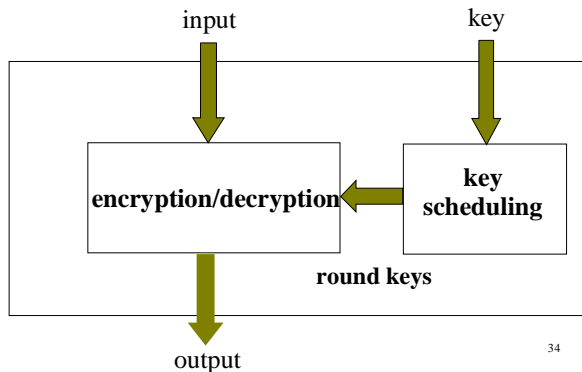
32

Design of S-boxes

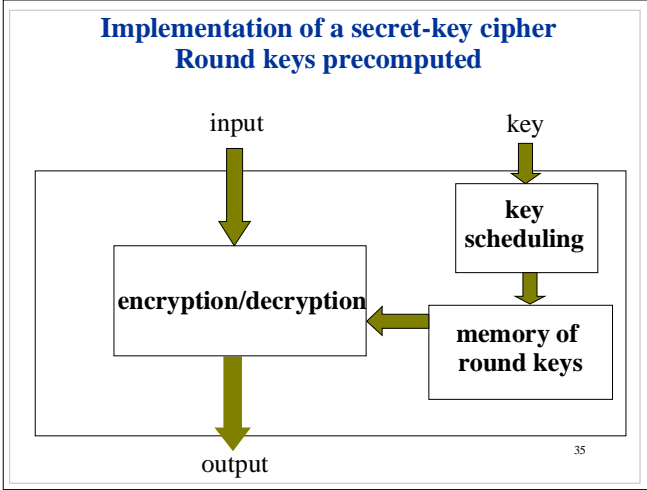


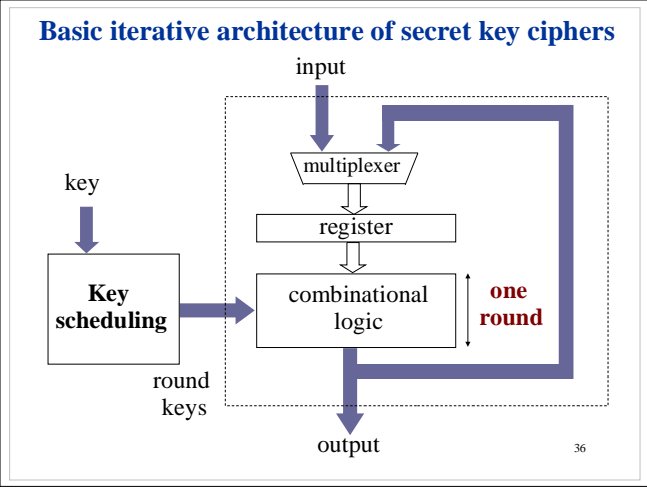
- $16! \approx 2 \cdot 10^{13}$ possibilities
- precisely defined initially unpublished criteria
- resistant against differential cryptanalysis (attack known to the designers and rediscovered in the open research in 1990 by E. Biham and A. Shamir)

Implementation of a secret-key cipher in hardware Round keys computed on-the-fly



34





Properties and security of DES

37

Theoretical design of the specialized machine to break DES

Project: Michael Wiener, Entrust Technologies, 1993, 1997

Method: **exhaustive key search attack**

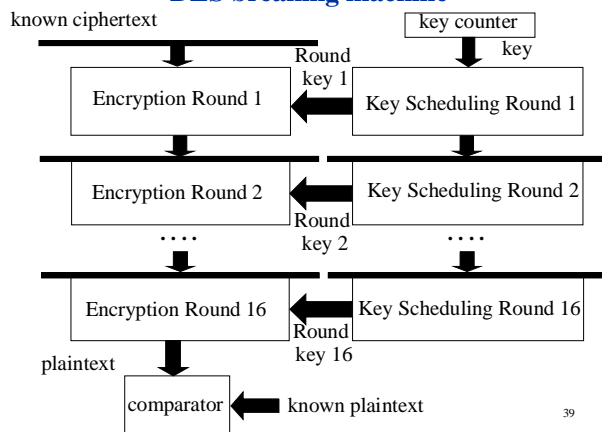
Basic component: specialized integrated circuit in CMOS technology, 75 MHz

Checks: 200 mln keys per second
Costs: \$10

Total cost	Estimated time
\$ 1 mln	35 minutes
\$ 100.000	6 hours

38

DES breaking machine

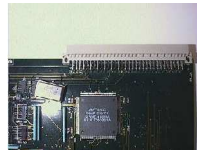


39

Deep Crack

Electronic Frontier Foundation, 1998

Total cost: \$220,000
Average time of search: 4.5 days/key



1800 ASIC chips, 40 MHz clock

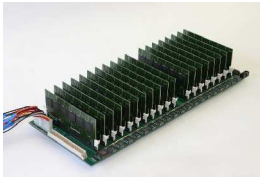
40

Deep Crack

Parameters

Number of ASIC chips	1800
Clock frequency	40 MHz
Number of clock cycles per key	16
Number of search units per ASIC	24
Search speed	90 bln keys/s
Average time to recover the key	4.5 days ₄₁

Copacobana



- Since 2006
- FPGA based
- Massive Parallel
- Total Cost: 9.000€ (12,600\$)
- Average Search Time: 6.4 days
- Reprogramable etc. target ECC
- Horst Görtz Institute for IT-Security, Germany⁴²

Minimum length of the key for symmetric ciphers

I. Panel of experts, January 1996

M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, M. Wiener

Report:

“Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security”

II. National Academy of Sciences, National Research Council, May 1996

Report:

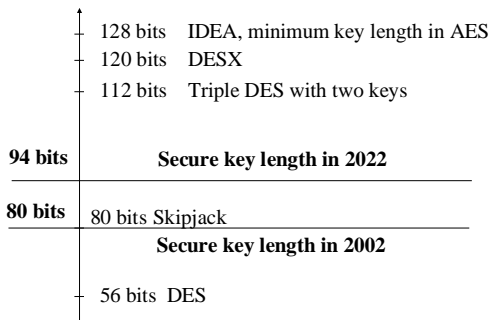
“Cryptography’s Role in Securing the Information Society”

Minimum key length for symmetric-key ciphers (2000)
 new timings based on Copacabana (2007)

Intruder	Budget	Tools	Time		Secure key length
			40 bits	56 bits	
Hacker	tiny	PC	1 week	infeasible	45
Small business	\$400	FPGA	5 hrs	38 years	50
	\$10,000	FPGA	12 min	18 months 6.4 days	55
Corporate department	\$300 K	FPGA	24 sec	19 days 5 hours	60
		ASIC	18 sec	3 hrs	
Big company	\$10 M	FPGA	7 sec	13 hrs 9.2 min	70
		ASIC	5 ms	6 min	
Intelligence agency	\$300 M	ASIC	0.2 ms	12 sec	75 ₄₄
		FPGA		18 sec	

Secure key length today and in 20 years

key length



Secure key length - discussion

- increasing key length in a newly developed cipher costs NOTHING
- increasing effective key length, assuming the use of an existing cipher has a limited influence on the efficiency of implementation (DESX, Triple DES)

It is economical to use THE SAME secure key length FOR ALL applications

The primary barriers blocking the use of symmetric ciphers with a secure key length have been of the political nature (e.g., export policy of USA)

Other attacks

- **differential cryptanalysis**

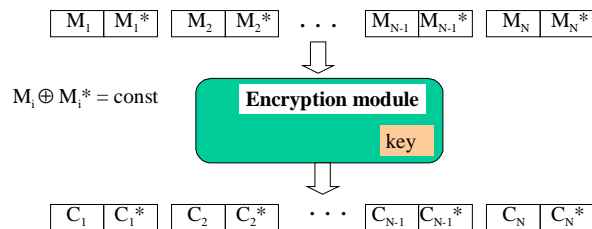
Biham, Shamir 1991

- **linear cryptanalysis**

Matsui, 1993

47

Differential cryptanalysis



- access to the encryption module with the key inside
- analysis of trillions of pairs plaintext-ciphertext

48

Differential cryptanalysis of DES

Biham, Shamir 1991

Requirements:

- **access to the encryption module** with the key inside
- time for encryption of $2^{47} = 1,4 \cdot 10^{14}$ plaintext blocks
= **1 million gigabytes of plaintext**

Conclusions:

- **attack impossible** to mount
- DES **specially designed** (IBM, NSA) to be resistant against differential cryptanalysis

49

What if creators of DES did not know about differential cryptanalysis...

Required number of plaintext blocks

Original DES $2^{47} = 1 \text{ mln GB}$

Modifications:

Identity permutation in place of P $2^{19} = 4 \text{ MB}$

Order of S-boxes $2^{38} = 2,000 \text{ GB}$

XOR replaced by addition $2^{31} = 2 \text{ GB}$

S-boxes random one position changed $2^{21} = 16 \text{ MB}$
 $2^{33} = 8 \text{ GB}$

Expansion function E eliminated $2^{26} = 64 \text{ MB}$ ⁵⁰

Differential and linear cryptanalysis - discussion

- Attacks **infeasible** for correctly designed ciphers
- Perfect **tool for comparing strengths** of various ciphers
- Resistance against these attacks does not imply resistance against other **unknown methods of attack**

51

RC5

52

RC5 *Ron Rivest, MIT, 1994*

(Ron's Code 5, Rivest's Cipher 5)

- **variable key length** (40 bits in the former export version, 128 bits to achieve the same strength as IDEA)
- **variable block size** (depends on the processor word length)
- **variable number of rounds** (determines resistance to linear and differential cryptanalysis; for 9 rounds this resistance is greater than for DES)
- **simplicity of description**

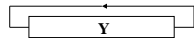
53

RC5

One of the fastest ciphers

Basic operation

Rotation by a variable number of bits



$Y = Y \ll X$

54

RC5 w/r/b

w - word size in bits $w = 16, 32, 64$

input/output block = 2 words = $2 \cdot w$ bits

Typical value:

$w=32 \Rightarrow$ 64-bit input/output block

r - number of rounds

b - key size in bytes $0 \leq b \leq 255$

key size in bits = $8 \cdot b$ bits

Recommended version: RC5 32/12/16

64 bit block

12 rounds

128 bit key

55

RC5

Encryption

```

A || B = M
A = A + S[0]
B = B + S[1]
for i= 1 to r do
{
  A= ((A⊕B) <<< B) + S[2i]
  B= ((B⊕A) <<< A) + S[2i+1]
}
C= A || B
    
```

Decryption

```

A || B = C
for i= r downto 1 do
{
  B= ((B-S[2i+1]) >>> A) ⊕ A
  A= ((A - S[2i])>>>B) ⊕ B
}
B = B - S[1]
A = A - S[0]
M= A || B
    
```

56

RC5 - Key Scheduling

k bits of the main key



$2 \cdot r + 2$ round keys = $(2 \cdot r + 2) \cdot w$ bits

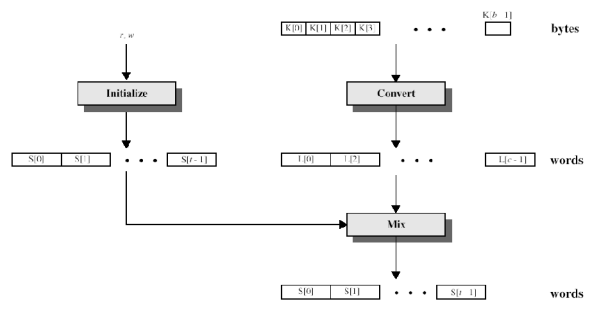
Two magic constants:

$P_w = \text{Odd}((e-2) \cdot 2^w)$ e - base of natural logarithms
 $e = 2.7182\dots$

$Q_w = \text{Odd}((\phi-1) \cdot 2^w)$ ϕ - golden ratio

$$\phi - \text{golden ratio} = \frac{x}{y} = \frac{y}{x-y} = 1.6180\dots$$

RC5 - Key Scheduling



58

RC5 - Key Scheduling Initialize and Convert

Initialize

$S[0] = P_w$
 for $i=1$ to $t-1$ do
 $S[i] = S[i-1] + Q_w$

$$t = 2 \cdot r + 2$$

Convert

for $i=0$ to $c-1$ do
 $L[i] = 0;$

$$c = \left\lceil \frac{8 \cdot b}{w} \right\rceil$$

Copy key bits directly to the memory positions represented by L.

59

RC5 - Key Scheduling Mix

Mix

$i = j = 0$
 $A = B = 0$
 do $3 \cdot \max\{t, c\}$ times
 {
 $A = S[i] = (S[i] + A + B) \lll 3$
 $B = L[j] = (L[j] + A + B) \lll (A+B)$
 $i = (i+1) \bmod t$
 $j = (j+1) \bmod c$
 }

60

RC5 - Resistance to differential and linear cryptanalysis

Plaintext requirement

# rounds	4	5	6	7	9	12	13
Differential Cryptanalysis	2^{22}	2^{26}	2^{32}	2^{37}	2^{46}	2^{63}	$>2^{64}$
Linear Cryptanalysis	2^{37}	2^{47}	2^{57}	$>2^{64}$			

Differential cryptanalysis cannot be applied to RC5 with #rounds ≥ 13

Linear cryptanalysis cannot be applied to RC5 with #rounds $\geq 7_1$

Resistance of modern ciphers against known attacks

Proprietary ciphers built in application software	mostly insecure, seconds on PC
Proprietary ciphers with unknown specification	uncertain, impossible to verify
40-bit "international" version of ciphers	Keys recoverable using several hours with a small network of computers
DES	Keys can be recovered within 24 hours using a specialized machine worth about \$300,000
Triple DES, DESX, RC5, IDEA	All known attacks impractical

State of research regarding the security of secret-key ciphers

- limited number of researchers actively involved in cryptanalysis and design of new ciphers
- number of published ciphers > number of researchers
- evaluations of the cipher strength given by designers typically unreliable

"Honest" cipher = the best known attack is an exhaustive key search attack

One can rely only on ciphers analyzed by a large group of qualified researchers
