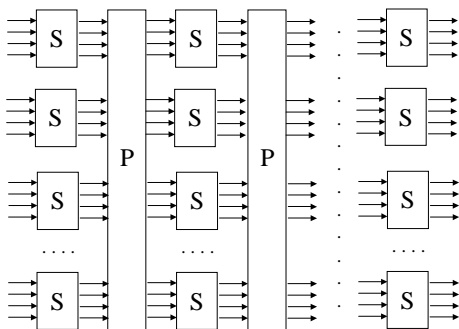


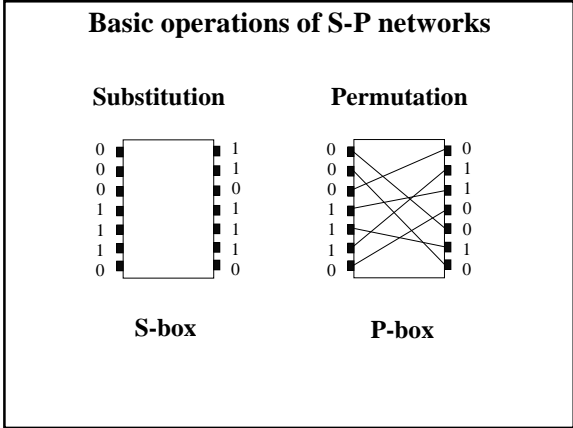
ECE297:11 Lecture 4

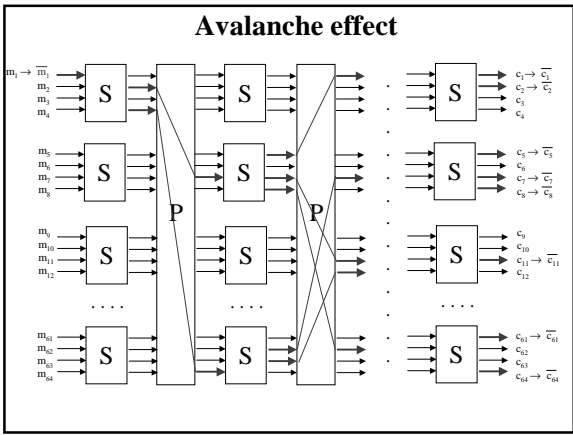
**Towards modern ciphers:
SP networks & DES**

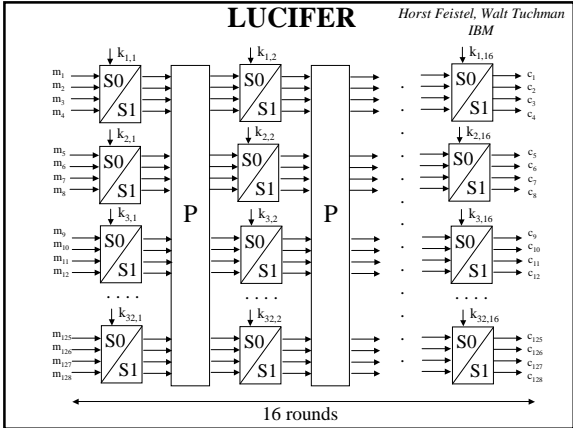
SP Networks

S-P Networks

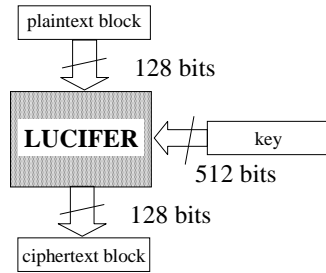








LUCIFER- external look



History of DES

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

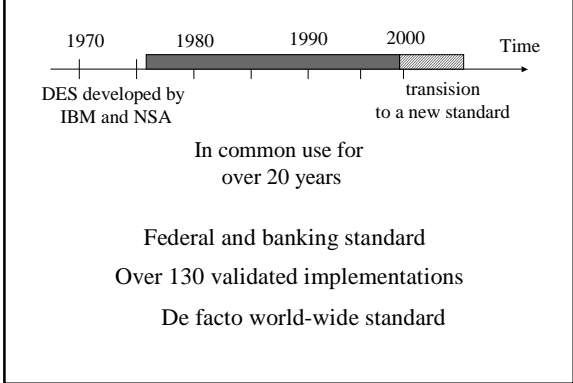
DES - chronicle of events

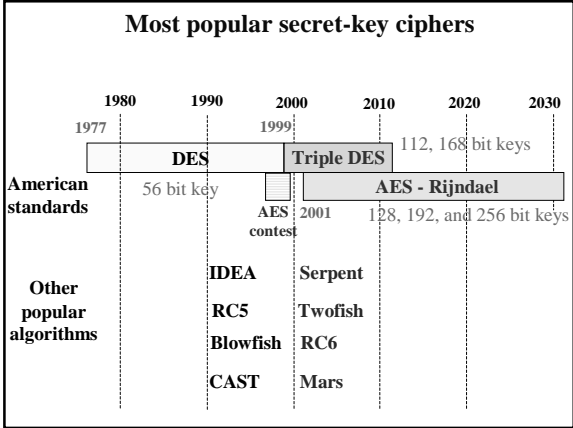
- 1973 - NBS issues a public request for proposals for a standard cryptographic algorithm
- 1975 - first publication of the IBM's algorithm and request for comments
- 1976 - NBS organizes two workshops to evaluate the algorithm
- 1977 - official publication as FIPS PUB 46: Data Encryption Standard
-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

Controversies surrounding DES

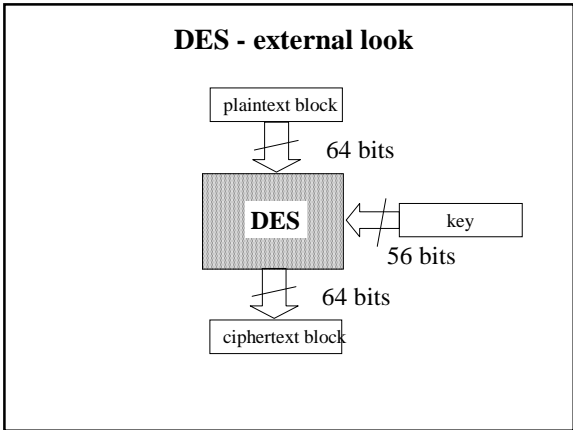
Unknown design criteria	Slow in software	Too short key
<p>Most criteria reconstructed from cipher analysis</p> <p>1990 Reinvention of differential cryptanalysis</p>	<p>Only hardware implementations certified</p> <p>1993 Software, firmware and hardware treated equally</p>	<p>Theoretical designs of DES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

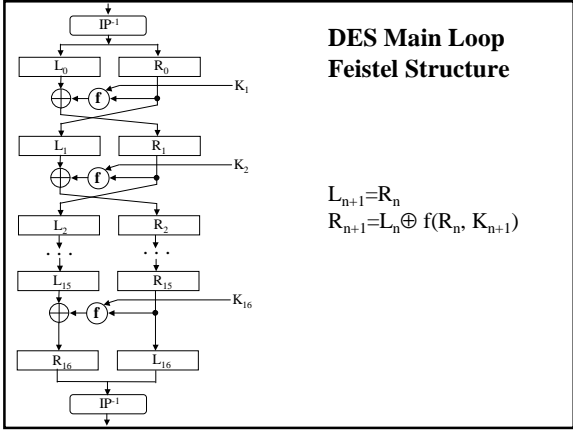
Life of DES

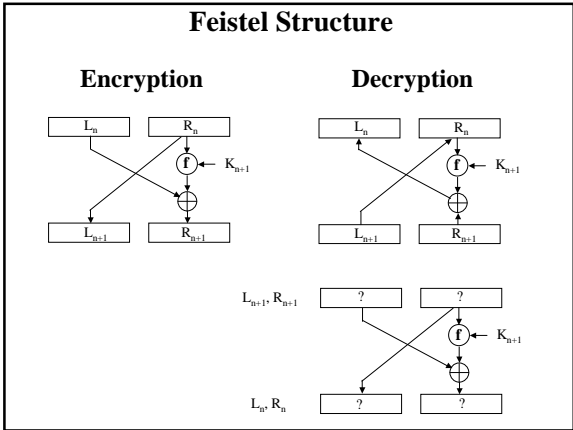


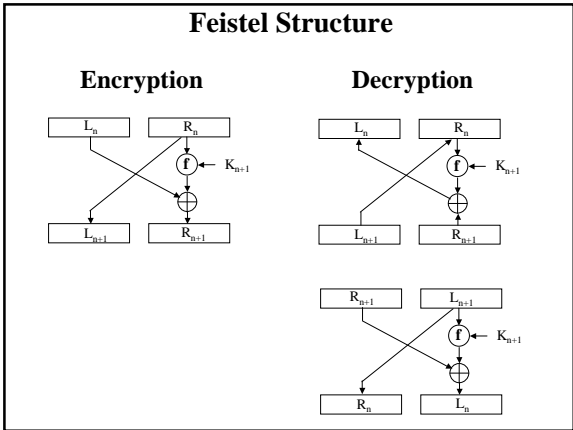


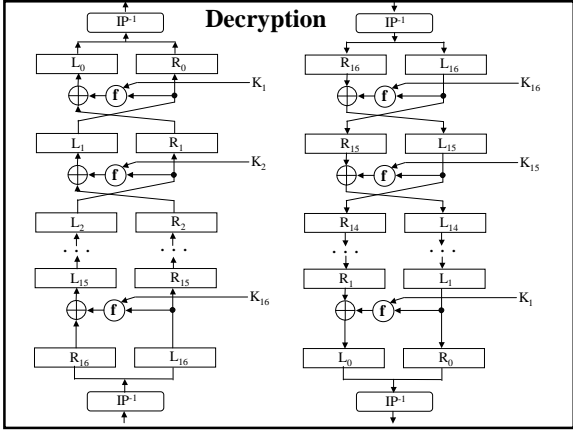
Specification of DES



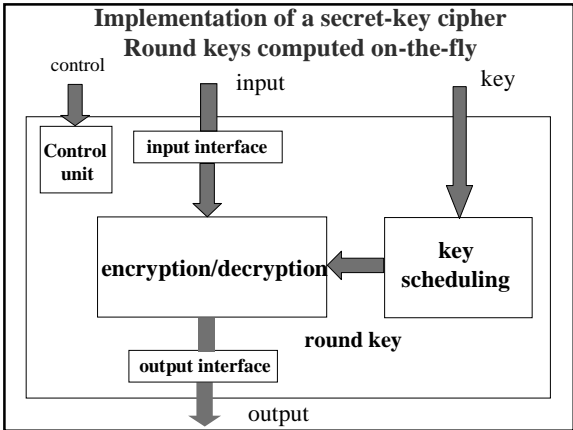


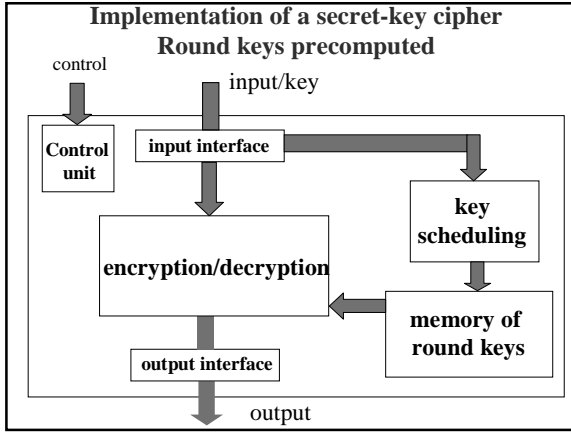


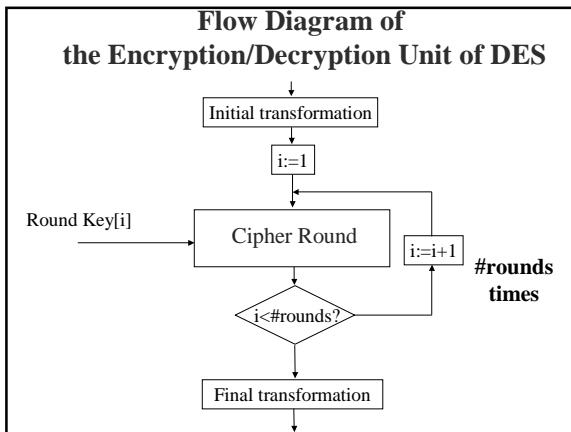


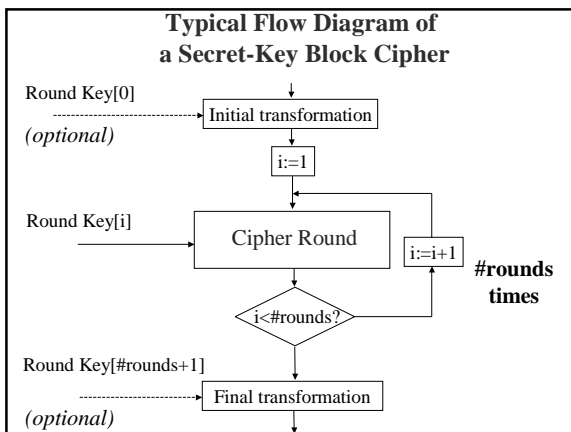


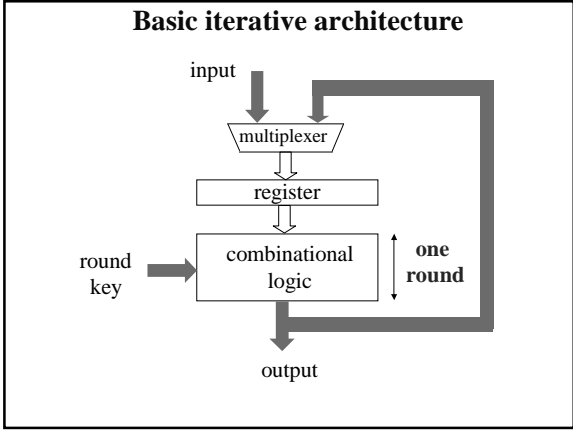
Implementing DES

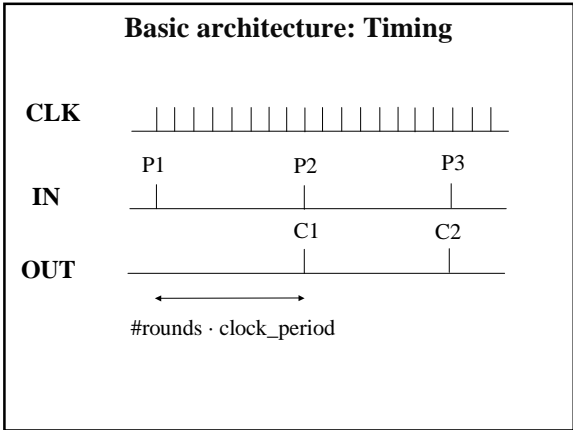


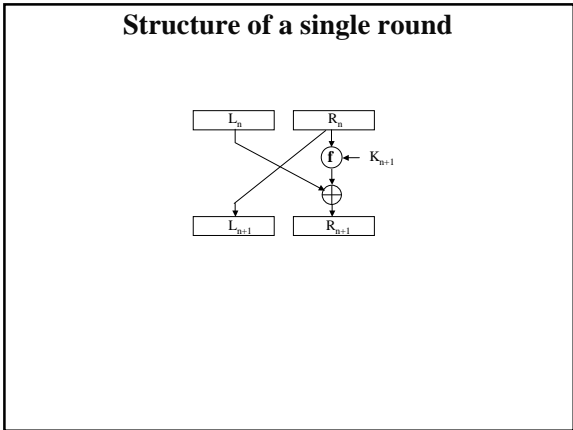


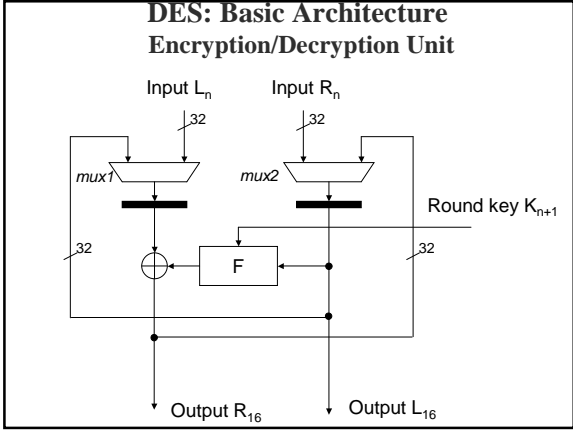


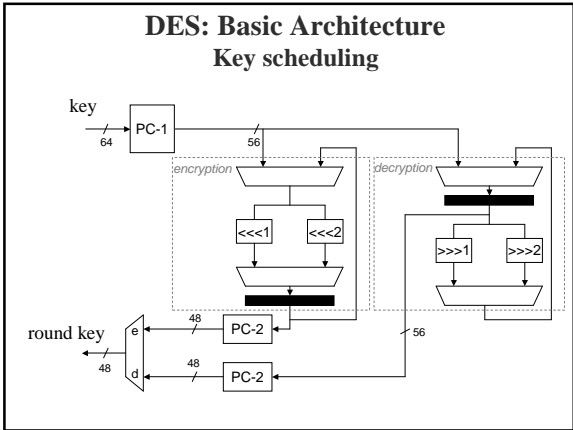












Breaking DES

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**

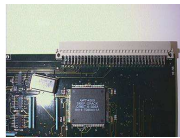
Costs: \$10

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

Deep Crack

Electronic Frontier Foundation, 1998

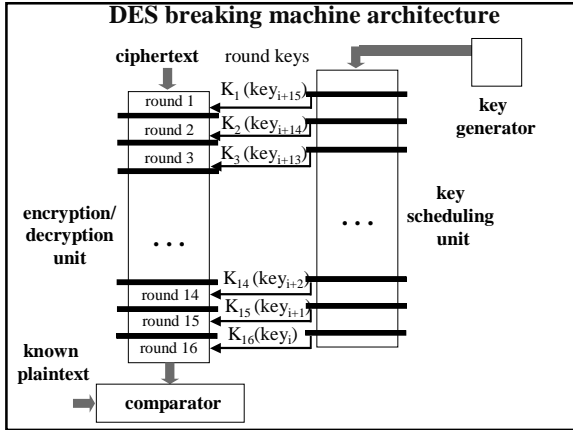
Total cost: \$220,000
Average time of search:
4.5 days/key



1800 ASIC chips, 40 MHz clock

**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



**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*

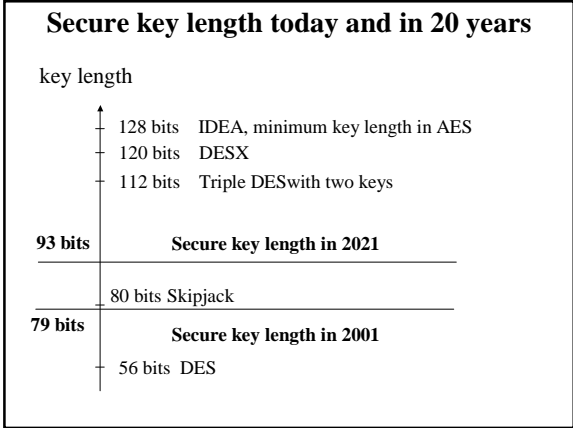
Report:
 "Minimal Key Lengths for Symmetric Ciphers
 to Provide Adequate Commercial Security"

**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

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	55
Corporate department	\$300 K	FPGA	24 sec	19 days	60
		ASIC	18 sec	3 hrs	
Big company	\$10 M	FPGA	7 sec	13 hrs	70
		ASIC	5 ms	6 min	
Intelligence agency	\$300 M	ASIC	0.2 ms	12 sec	75



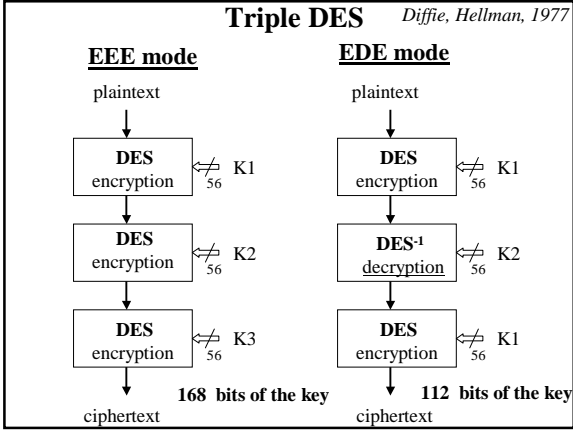
Secure key length - discussion

- 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)

Extensions of DES



Triple DES

Advantages:

- secure key length (112 or 168 bits)
- increased compared to DES resistance to linear and differential cryptanalysis
- possibility of utilizing existing implementations of DES

Disadvantages:

- relatively slow, especially in software

