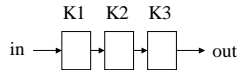


ECE 297:11 Lecture 7

Advanced Encryption Standard

Why a new standard?

1. Old standard insecure against brute-force attacks
2. Straightforward fixes lead to inefficient implementations

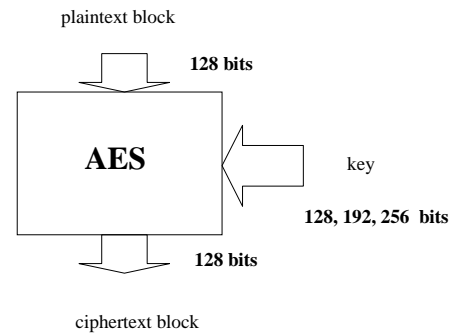
• Triple DES 

3. New trends in fast software encryption
 - use of basic instructions of the microprocessor
4. New ways of assessing cipher strength
 - differential cryptanalysis
 - linear cryptanalysis

Why a contest?

- Focus the effort of cryptographic community
 - Small number of specialists in the open research
- Stimulate the research on methods of constructing secure ciphers
- Avoid backdoor theories
- Speed-up the acceptance of the standard

External format of the AES algorithm



Rules of the contest

Each team submits

Detailed cipher description

Justification of design decisions

Tentative results of cryptanalysis

Source code in C

Source code in Java

Test vectors

AES Contest Effort

June 1998

15 Candidates

from USA, Canada, Belgium, France, Germany, Norway, UK, Israel, Korea, Japan, Australia, Costa Rica

Round 1

Security
Software efficiency

August 1999

5 final candidates

Mars, RC6, Rijndael, Serpent, Twofish

Round 2

Security
Hardware efficiency

October 2000

1 winner: Rijndael
Belgium

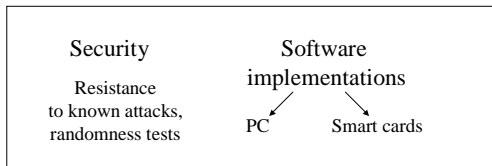
AES contest - First Round

- 15 June 1998** Deadline for submitting candidates
21 submissions,
15 fulfilled all requirements
- August 1998** 1st AES Conference in Ventura, CA
Presentation of candidates
- March 1999** 2nd AES Conference in w Rome, Italy
Review of results of the First Round
analysis
- August 1999** NIST announces five final candidates

AES: Candidate algorithms

North America (8)	Europe (4)	Asia (2)
Canada: CAST-256 Deal	Germany: Magenta	Korea: Crypton
USA: Mars RC6 Twofish Safer+ HPC	Belgium: Rijndael	Japan: E2
Costa Rica: Frog	France: DFC	Australia (1)
	Israel, GB, Norway: Serpent	Australia: LOKI97

First round June 1998-August 1999



Survey filled by 104 participants of the Second AES Conference in Rome, March 1999

1. Rijndael	+76	
2. RC6	+73	
3. Twofish	+61	Overwhelming YES
4. Mars	+52	
5. Serpent	+45	
6. E2	+14	Mild YES
7. CAST-256	-2	
8. Safer+	-4	Middle-of-the-Road
9. DFC	-5	
10. Crypton	-15	Mild NO
11. DEAL	-70	
12. HPC	-77	
13. Magenta	-83	Overwhelming NO
14. Loki97	-85	
15. Frog	-85	

AES Finalists (1)

USA

Mars - IBM

C. Burwick, D. Coppersmith, E. D'Avignon,
R. Gennaro, S. Halevi, C. Jutla, S. M. Matyas,
L. O'Connor, M. Peyravian, D. Safford,
N. Zunic

RC6 - RSA Data Security, Inc.

R. Rivest - MIT
M. Robshaw, R. Sidney, Y. L. Yin - RSA

Twofish - Counterpane Systems

B. Schneier, J. Kelsey, C. Hall, N. Ferguson
- Counterpane, D. Whiting - Hi/fn,
D. Wagner - Berkeley

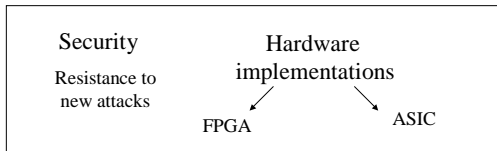
AES Finalists (2)

Europe

Rijndael - J. Daemen, V. Rijmen
Katholieke Universiteit Leuven
Belgium

Serpent - R. Anderson, Cambridge, England
E. Biham - Technion, Israel
L. Knudsen, University of Bergen, Norway

Second round August 1999-August 2000



AES contest: Second Round

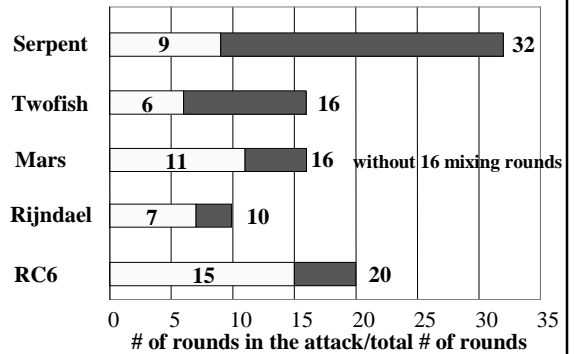
- 13-14 April 2000
3rd AES Conference in New York
- 15 May 2000
End of the comment period for Round II
- 2 October 2000 Winner announced**
- November 2001 FIPS-197: AES announced
- May 2002 Standard becomes effective

How NIST has made a final decision?

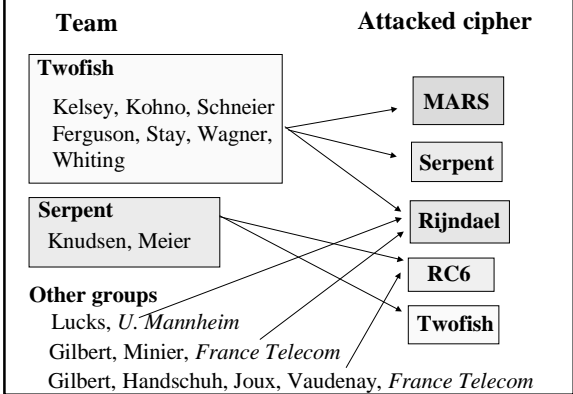
BASIC CRITERIA =

- security
- software efficiency
- hardware efficiency
- flexibility

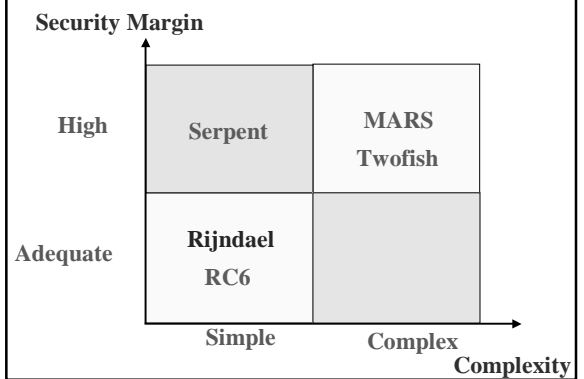
Security: Theoretical attacks better than exhaustive key search

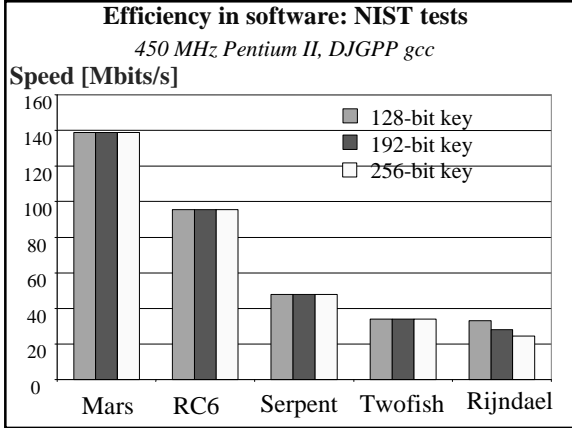
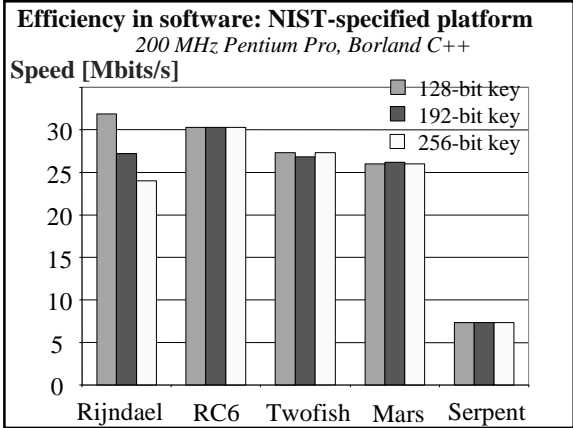


Security: Authors of attacks



NIST Report: Security





Efficiency in software: Ranking of encryption speeds for various platforms

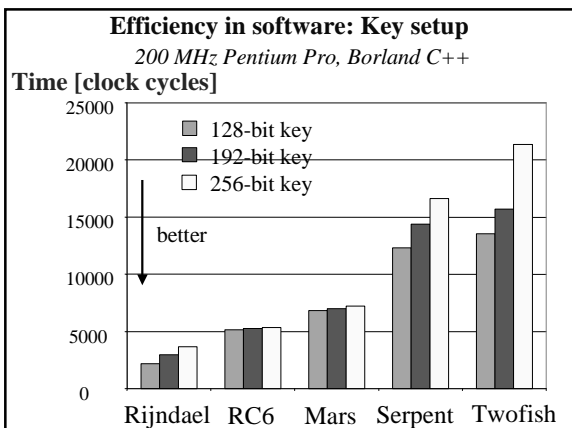
	Intel				Alpha		Sun-Sparc		H-P		
Mars	4	4	2	4	3	4	4	3	3	3	
RC6	1	3	1	1	4	1	4	3	3	5	4
Twofish	2	1	3	2	1	4	2	2	2	2	2
Rijndael	3	2	4	3	2	3	1	1	1	1	1
Serpent	5	5	5	5	5	5	5	5	5	4	5

NIST Report: Software Efficiency
Encryption and Decryption Speed

	32-bit processors	64-bit processors	DSPs
high	RC6	Rijndael Twofish	Rijndael Twofish
medium	Rijndael Mars Twofish	Mars RC6	Mars RC6
low	Serpent	Serpent	Serpent

NIST Report: Software Efficiency
Encryption and decryption speed in software on smart cards

	8-bit processors	32-bit processors
high	Rijndael	Rijndael RC6
medium	RC6 Mars Twofish	Mars
low	Serpent	Twofish Serpent



NIST Report: Software Efficiency
Key scheduling

	32-bit processors	64-bit processors	DSPs
high	Rijndael	Rijndael	Rijndael Serpent
medium	Mars RC6	RC6 Serpent	Mars RC6
low	Serpent Twofish	Mars Twofish	Twofish

NIST Report: Software Efficiency
Key scheduling on smart cards

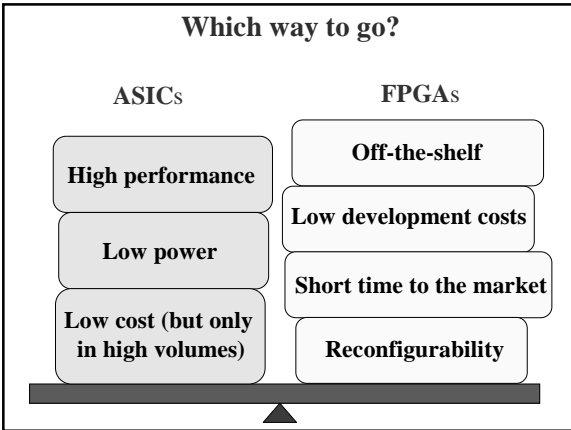
	8-bit processors
high	Rijndael
medium	Mars Twofish
low	RC6 Serpent

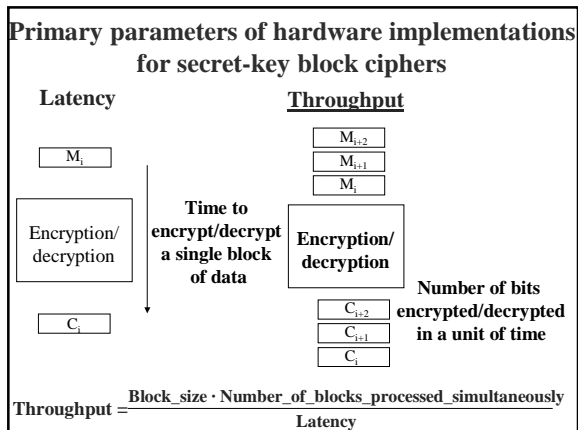
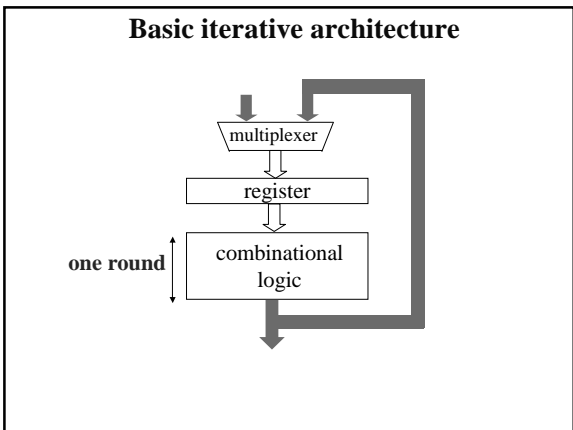
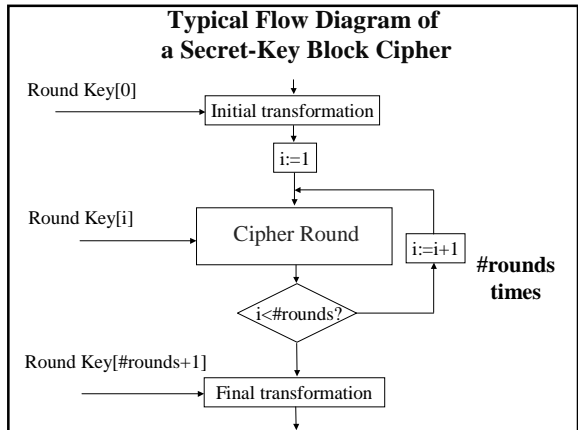
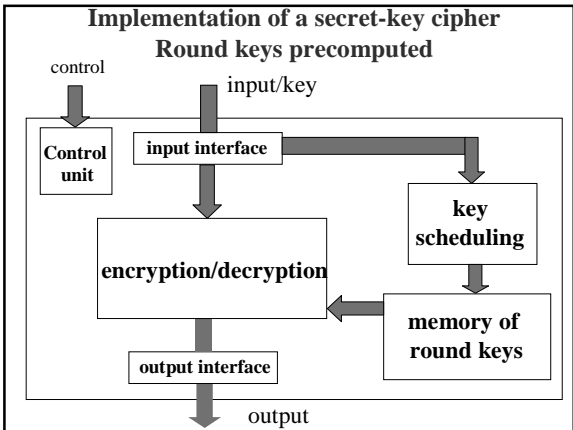
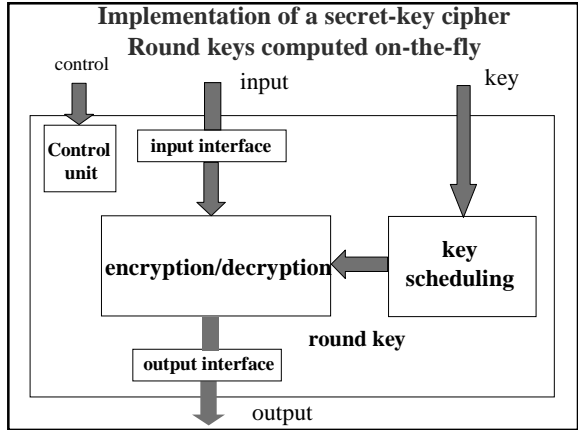
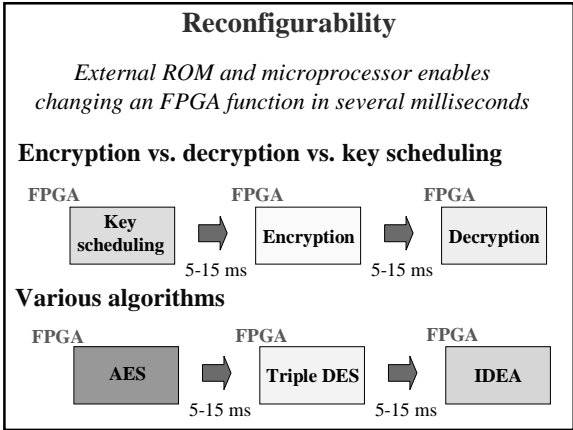
- Efficiency in software**
- Strong dependence on:**
1. Instruction set architecture (e.g., variable rotations)
 2. Programming language (assembler, C, Java)
 3. Compiler
 4. Programming style

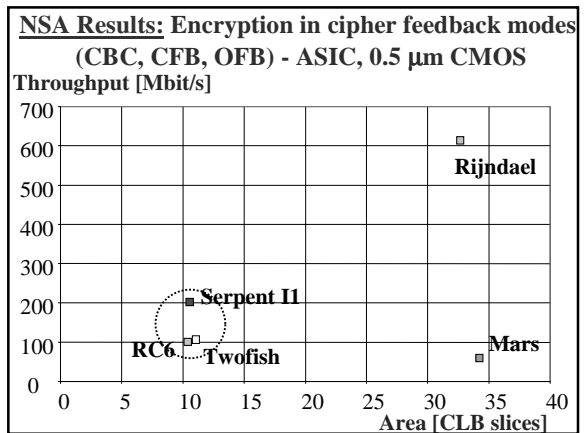
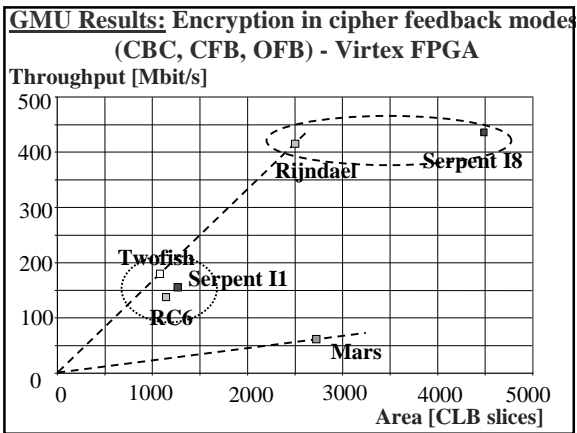
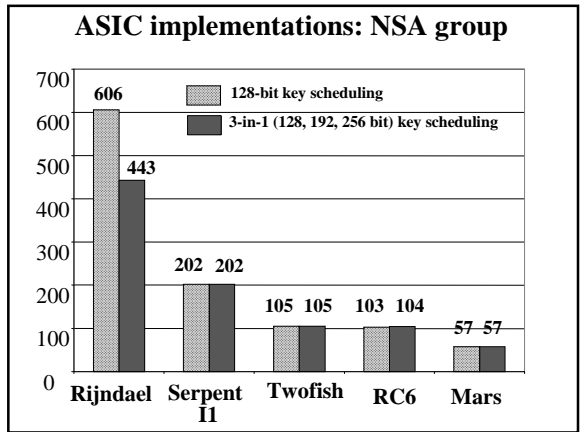
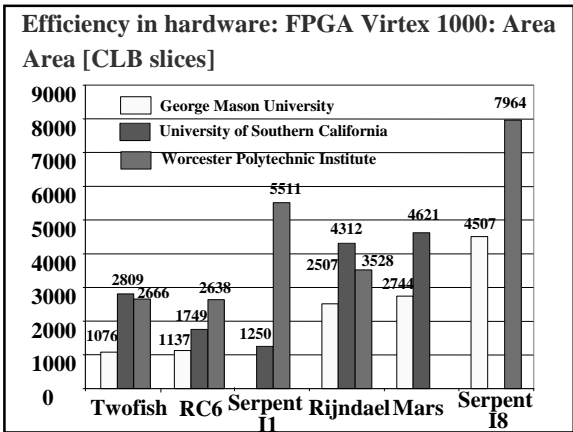
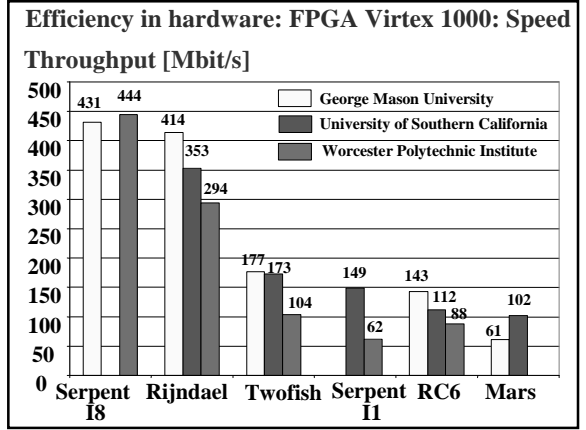
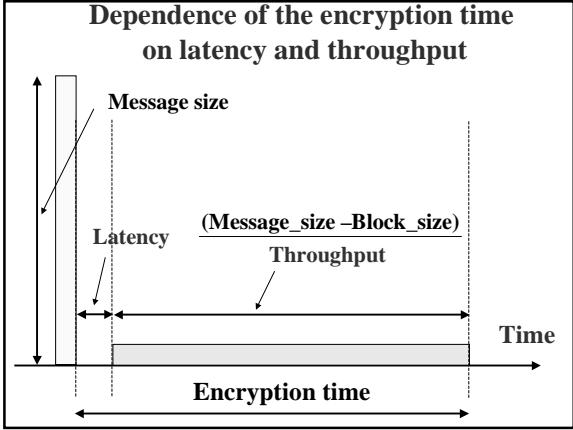
- Efficiency in software: Conclusions**
- Encryption/decryption**
- Strong variation of results
- Serpent the worst for majority of platforms
- Key setup**
- Moderate variation of results
- Rijndael and RC6 the best for majority of platforms
- Twofish and Serpent the worst for majority of platforms

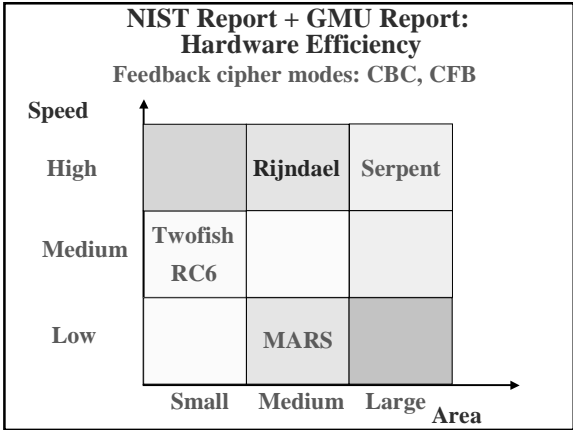
Primary ways of implementing cryptography in hardware

ASIC Application Specific Integrated Circuit	FPGA Field Programmable Gate Array
<ul style="list-style-type: none"> • designs must be sent for expensive and time consuming fabrication in semiconductor foundry • designed all the way from behavioral description to physical layout 	<ul style="list-style-type: none"> • bought off the shelf and reconfigured by designers themselves • no physical layout design; design ends with a bitstream used to configure a device







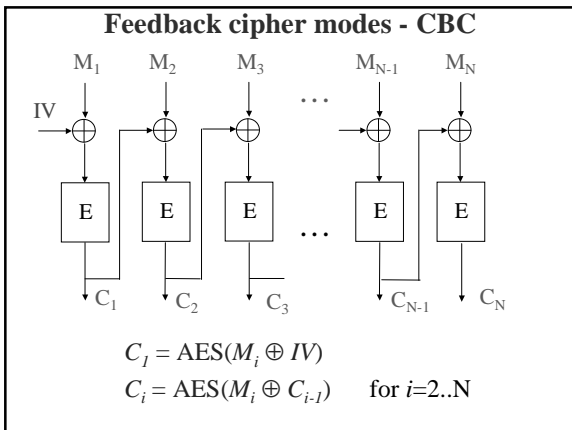
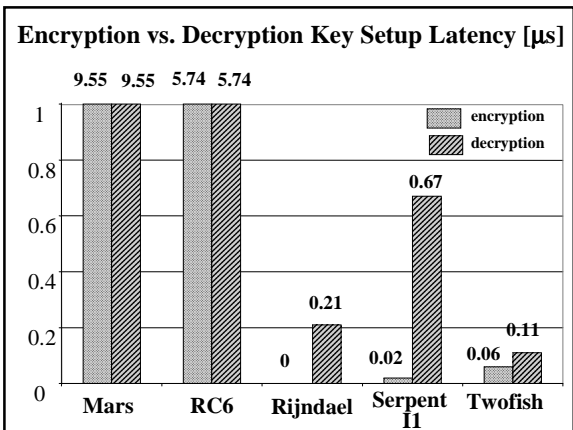
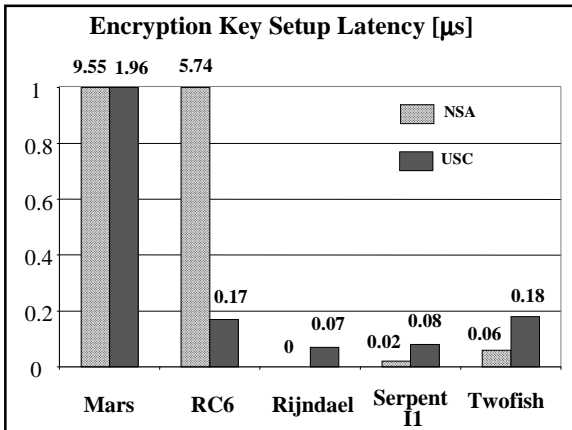


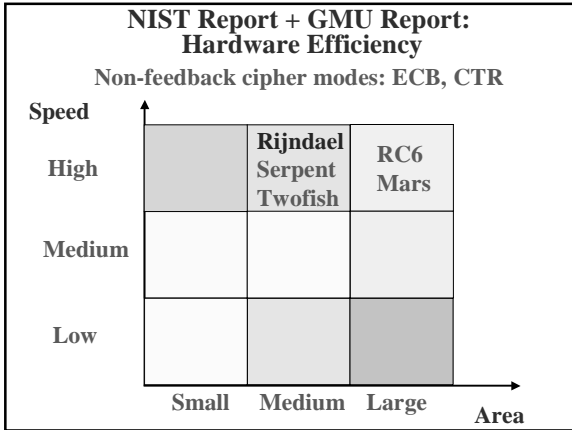
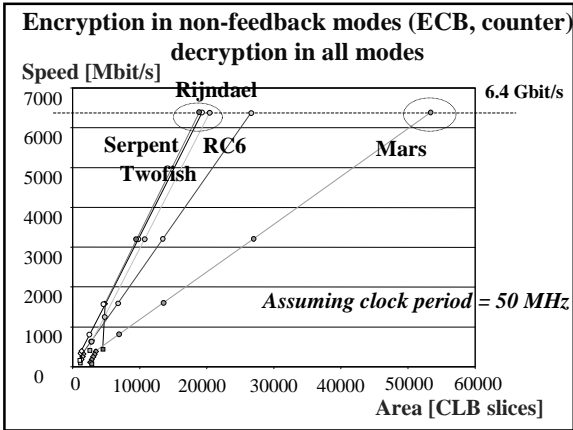
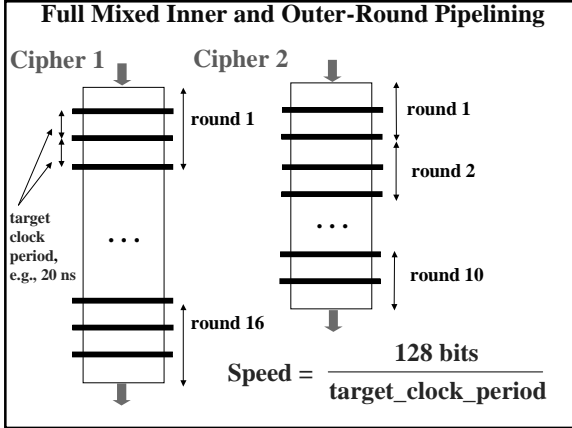
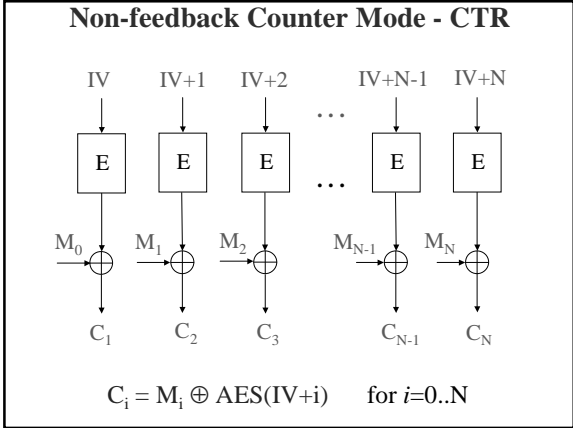
**Conclusions for feedback cipher modes (1)
(CBC, CFB, OFB)**

- Speed (throughput) should be the primary criteria of comparison
- Basic iterative architecture is the most appropriate for comparison and future implementations
- Serpent and Rijndael are over twice as fast as the next best candidate for all implementations

**Conclusions for feedback cipher modes (2)
(CBC, CFB, OFB)**

- Results confirmed by
 - three independent university groups for FPGAs, and
 - NSA group for ASICs
- Results of comparison independent of implementation technology (FPGAs vs. ASICs)





Conclusions for non-feedback cipher modes (1) ECB, counter

- All ciphers can achieve approximately the same speed.
Area should be the primary criteria of comparison.
- Serpent, Twofish and Rijndael are the most cost-efficient and take approximately the same amount of area

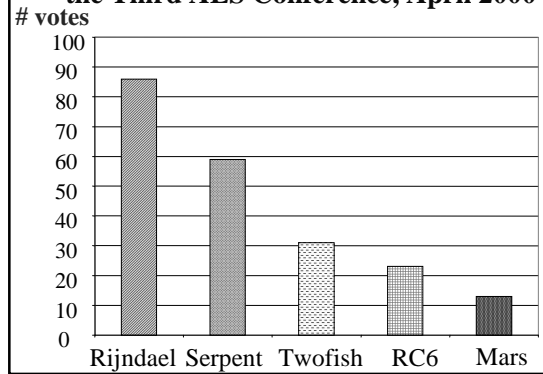
Importance of the AES candidate hardware efficiency comparison

- Important factor used to differentiate among final candidates
 - objective and commonly accepted measures
 - good agreement among results from various groups
 - large differences among final candidates
- Efficient architectures and methodologies developed for all algorithms

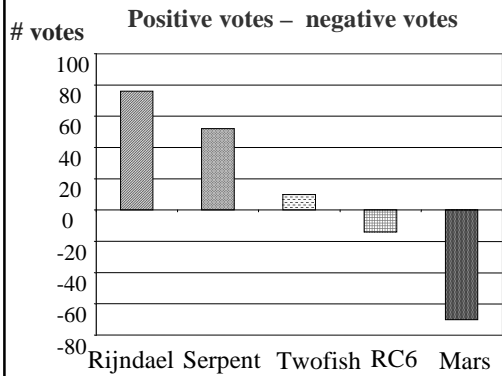
Flexibility: Criteria

- Additional key-sizes and block-sizes
- Ability to function efficiently and securely in a wide variety of platforms and applications
 - low-end smartcards, wireless - memory requirements
 - IPSec, ATM - key setup time in hardware
 - B-ISDN, satellite communication - encryption speed

Survey filled by 167 participants of the Third AES Conference, April 2000



Ranking by participants of the AES3 Conference



Most likely winner(s) (1)

Rijndael

- | | |
|--|---|
| + | - |
| <ul style="list-style-type: none"> • fastest in hardware • close to the fastest in software • very high flexibility | <ul style="list-style-type: none"> • security margin |
| novel ideas | |

Most likely winner(s) (2)

Serpent

- | | |
|--|--|
| + | - |
| <ul style="list-style-type: none"> • large security margin • conservative construction • very fast in hardware • cryptanalytical reputation of authors | <ul style="list-style-type: none"> • slow in software • moderate flexibility |

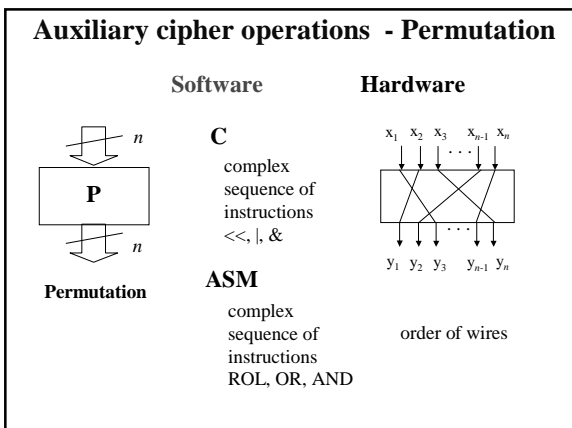
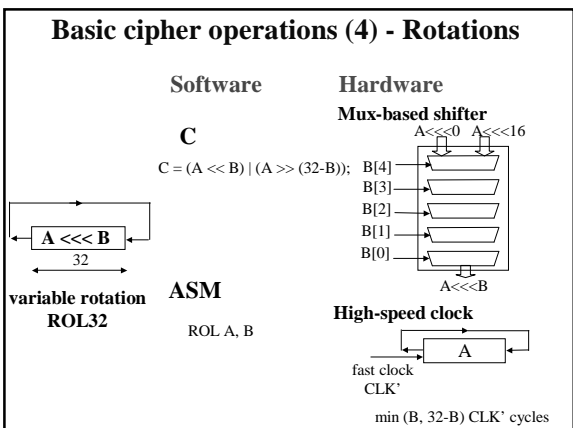
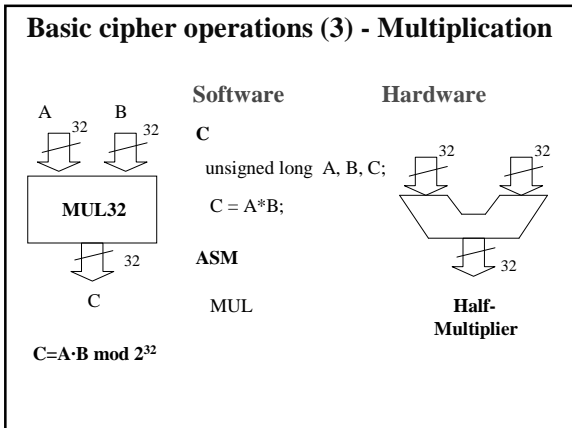
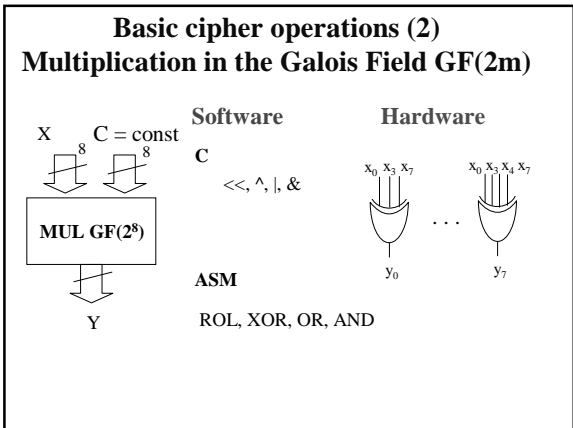
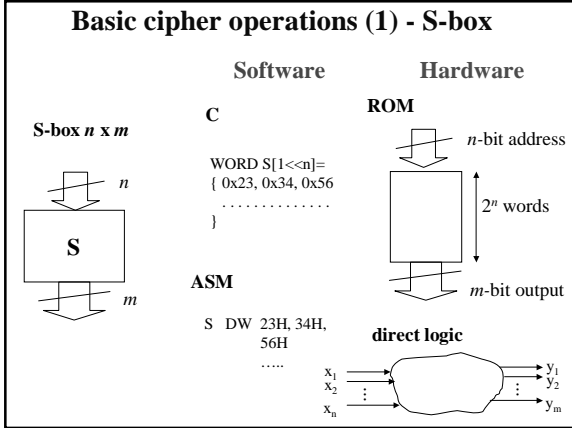
Most likely winner(s) (3)

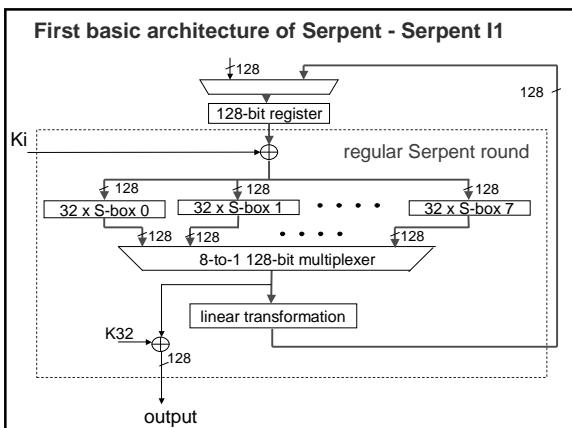
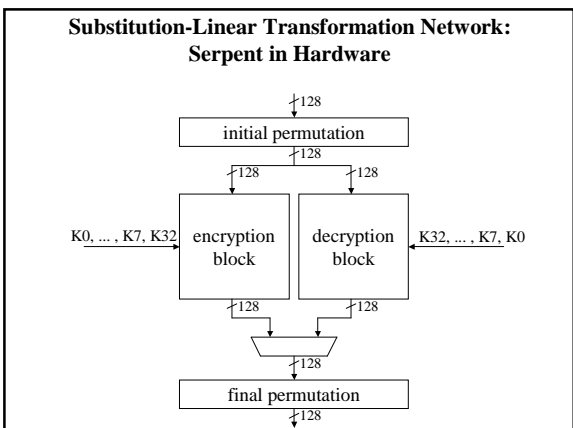
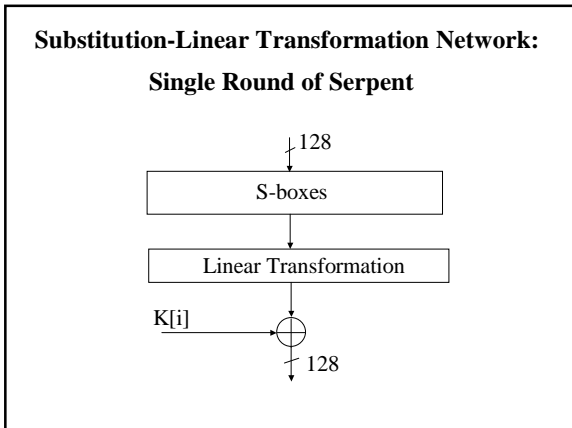
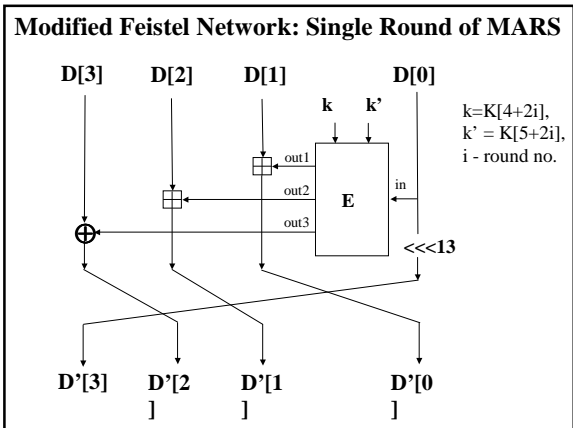
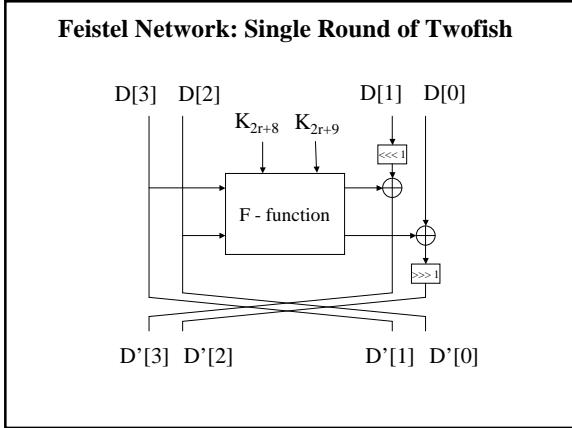
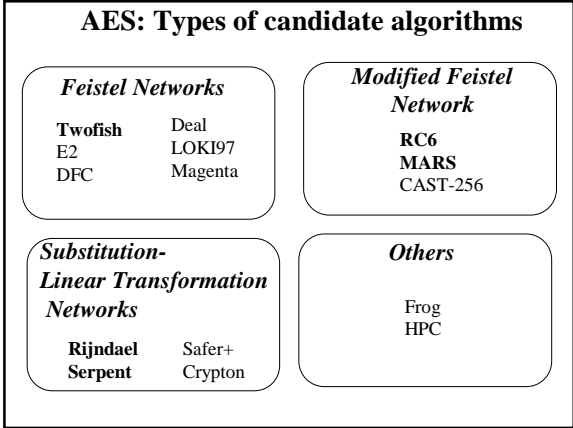
Twofish

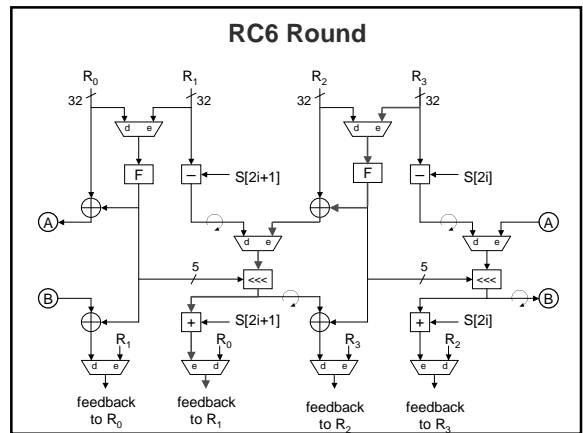
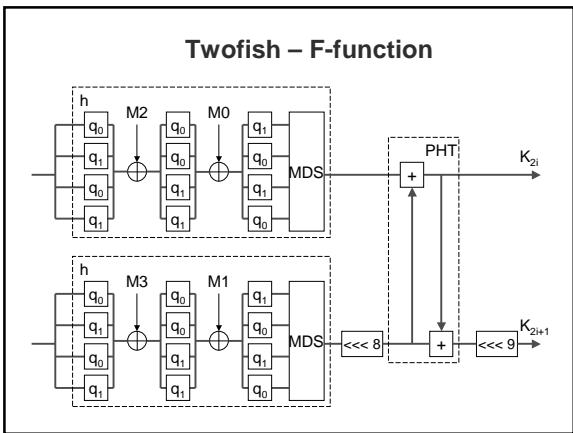
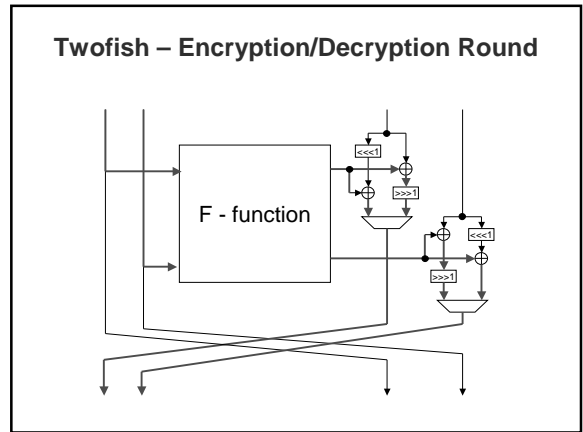
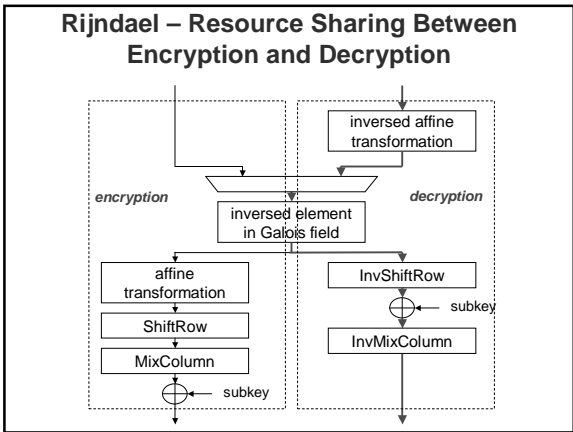
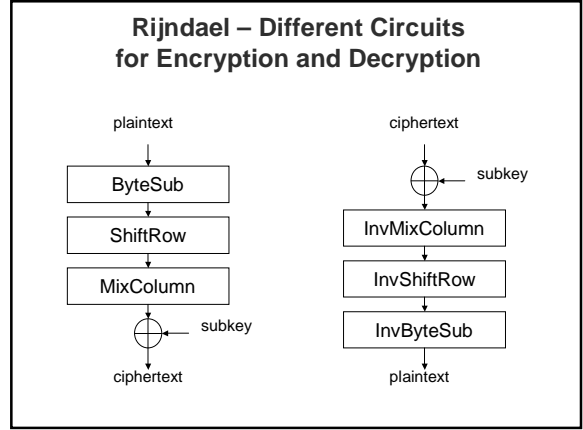
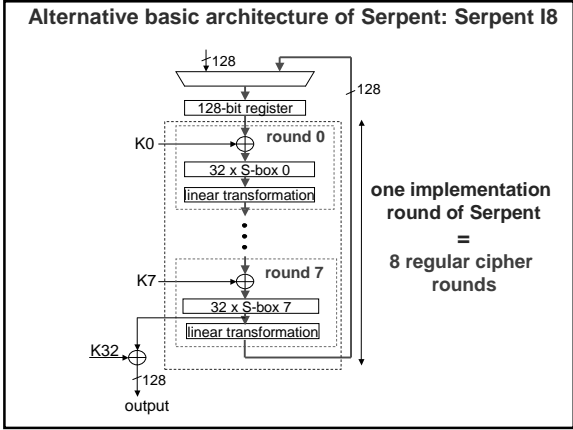
- | | |
|--|---|
| + | - |
| <ul style="list-style-type: none"> • good security margin • fast encryption/decryption in software | <ul style="list-style-type: none"> • moderately fast in hardware • slow key setup in software |
| <ul style="list-style-type: none"> • American • strongly advertized | <ul style="list-style-type: none"> • moderate flexibility |

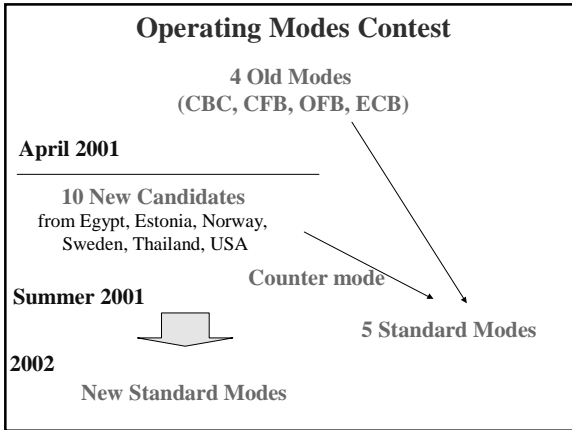
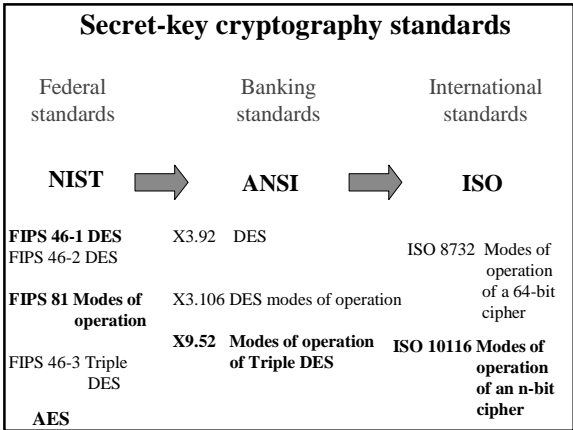
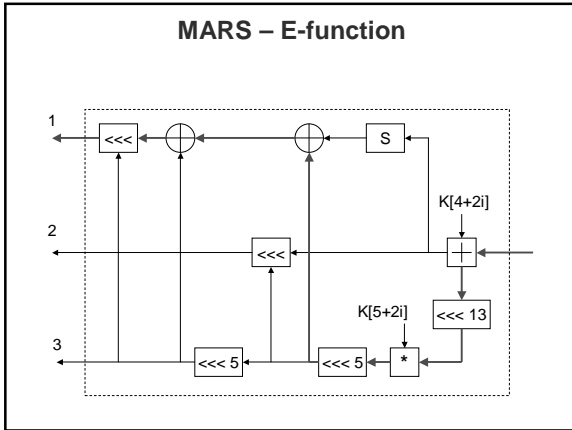
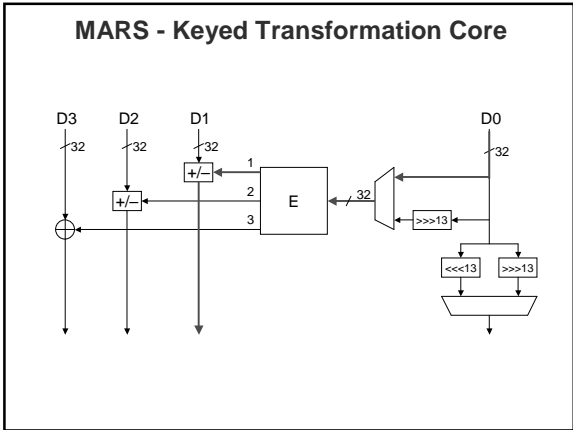
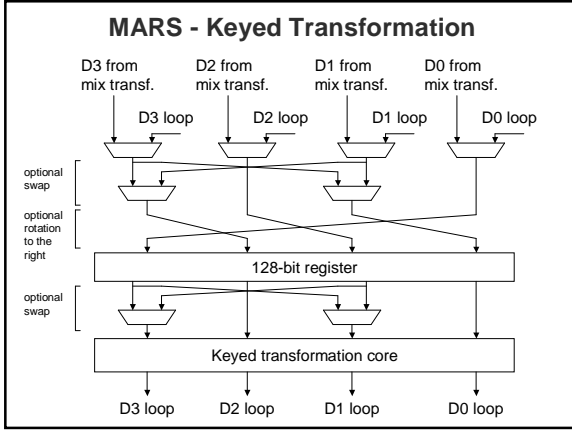
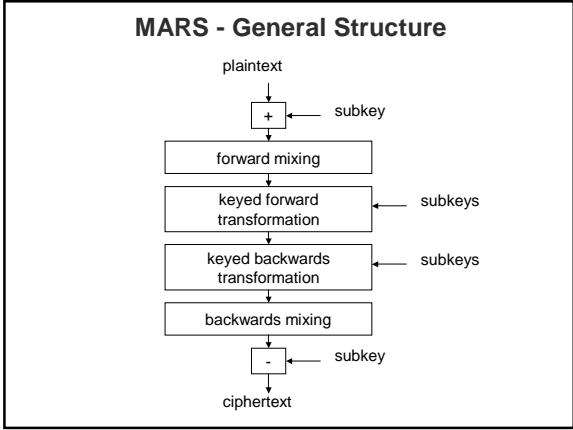
Major operations of AES finalists

	Serpent	Rijndael	Twofish	RC6	Mars
S-boxes					
Multiplication in GF(2 ^m)					
Integer multiplication					
Variable rotation					



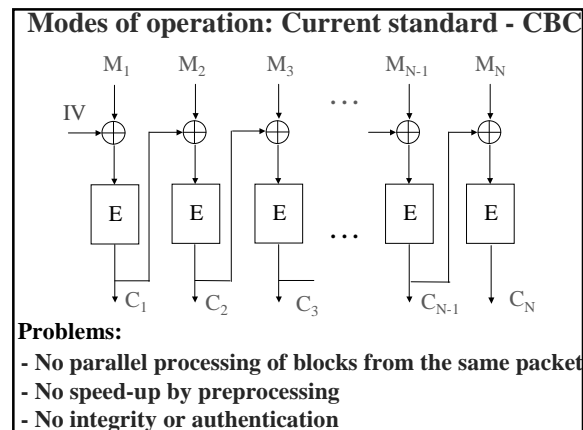
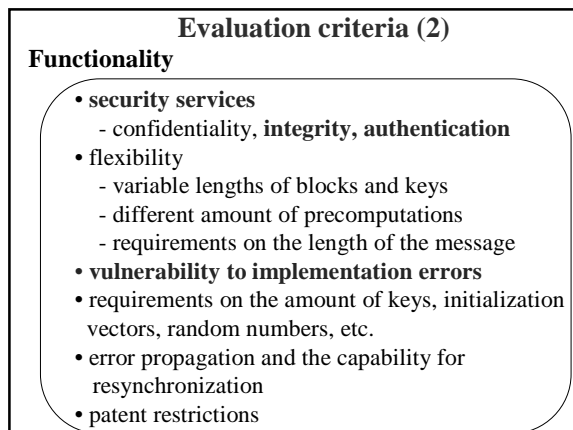
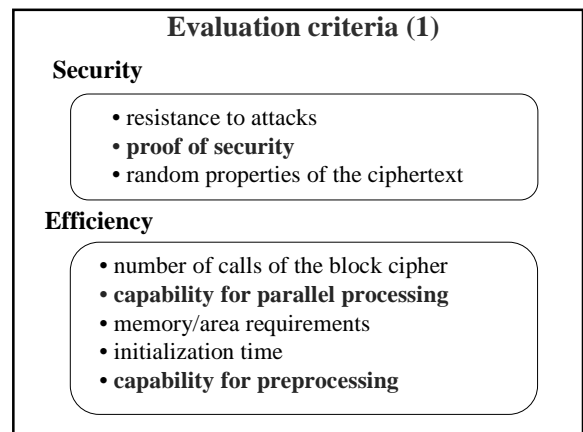
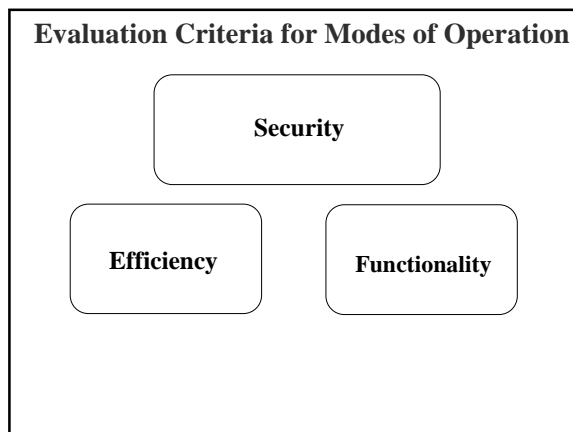


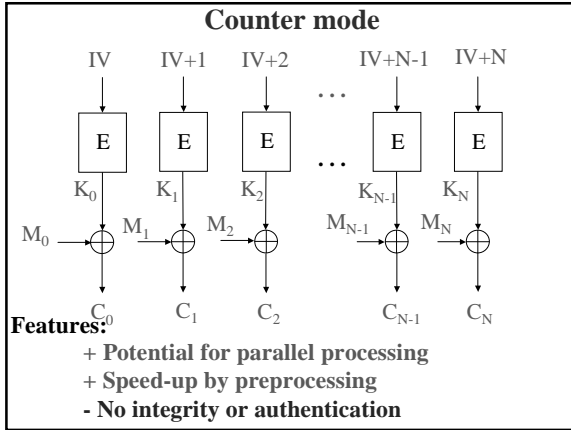




Modes submitted to the contest (1)			
	Full name	Authors	Institution
2DEM	2D-Encryption Mode	A. A. Belal, M. A. Abdel-Gawad	Alexandria University, Egypt
ABC	Accumulated Block Chaining	L. Knudsen	U. of Bergen Norway
CTR	Counter Mode	H. Lipmaa, P. Rogaway, D. Wagner	Finland, Estonia, USA, Thailand
IACBC	Integrity Aware CBC	C. Jutla	IBM, USA
IAPM	Integrity Aware Parallalizable Mode	C. Jutla	IBM, USA

Modes submitted to the contest (2)			
	Full name	Authors	Institution
IGE	Infinite Garble Extension	V. D. Gligor, P. Donescu	VDG, Inc., USA
KFB	Key Feedback Mode	J. Hästad, M. Naslund	NADA, Ericsson Sweden
OCB	Offset Codebook	P. Rogaway	UCSD, USA, Thailand
PCFB	Propagating Cipher Feedback	H. Hellström	StreamSec, Sweden
XCBC	eXtended CBC Encryption	V. D. Gligor, P. Donescu	VDG, Inc., USA





Properties of existing and new cipher modes				
	CBC	CFB	OFB	New standard
Proof of security	✓	✓	✓	✓
Parallel processing	decryption only		—	✓
Preprocessing	—	—	✓	✓
Integrity and authentication	—	—	—	✓
Resistance to implementation errors	✓	✓	—	✓

Encryption with authentication			
	Full name	Authors	Institutions
IACBC	Integrity Aware CBC	C. Jutla	IBM (patent)
IAPM	Integrity Aware Parallalizable Mode	C. Jutla	IBM (patent)
XCBC-XOR	eXtended CBC Encryption	V. D. Gligor, P. Donescu	VDG, Inc., (patent)
XECB-XOR	eXtended ECB Encryption	V. D. Gligor, P. Donescu	VDG, Inc., (patent)
OCB	Offset Codebook	P. Rogaway	UCSD, USA, Thailand

