AES (Advanced Encryption standard)

Approved in 2000 by US for civilian cryptographic use.

Approved in 2003 for classified and secret information.

NIST led 3 year approval process.

Solicited proposals, adopted AES from Europe.

AES used incorporated in standards, algorithms by IEEE, IETF, ISO and 3GPP.

DES (Digital Encryption Standard)

Forerunner to AES

1973 - NBS calls for proposals for block encryption standard.

A modified IBM proposal was adopted.

Orignal 128 bit key reduced to 56 bits.

Some changes to scrambling blocks.

concerns made because of differential cryptanalysis to make DES stronger?

2004 NIST withdrew DES,

Triple DES still approved for a while

(3 keys.

Choosing AES

DES suited for hardware, not software.

Software encryption more important.

AES requirements:

✓ Block Cipher

✓ At least as secure as triple DES

✓ 128 bit block size

✓ Key Size Options: 128, 192 and 256 bits.

✓ Unclassified and Open to Public (no PATENTS).

Fifteen proposals, in 1999 five final candidates

✓ MARS from IBM (US)

✓ RC6 from RSA Data Systems (USA)

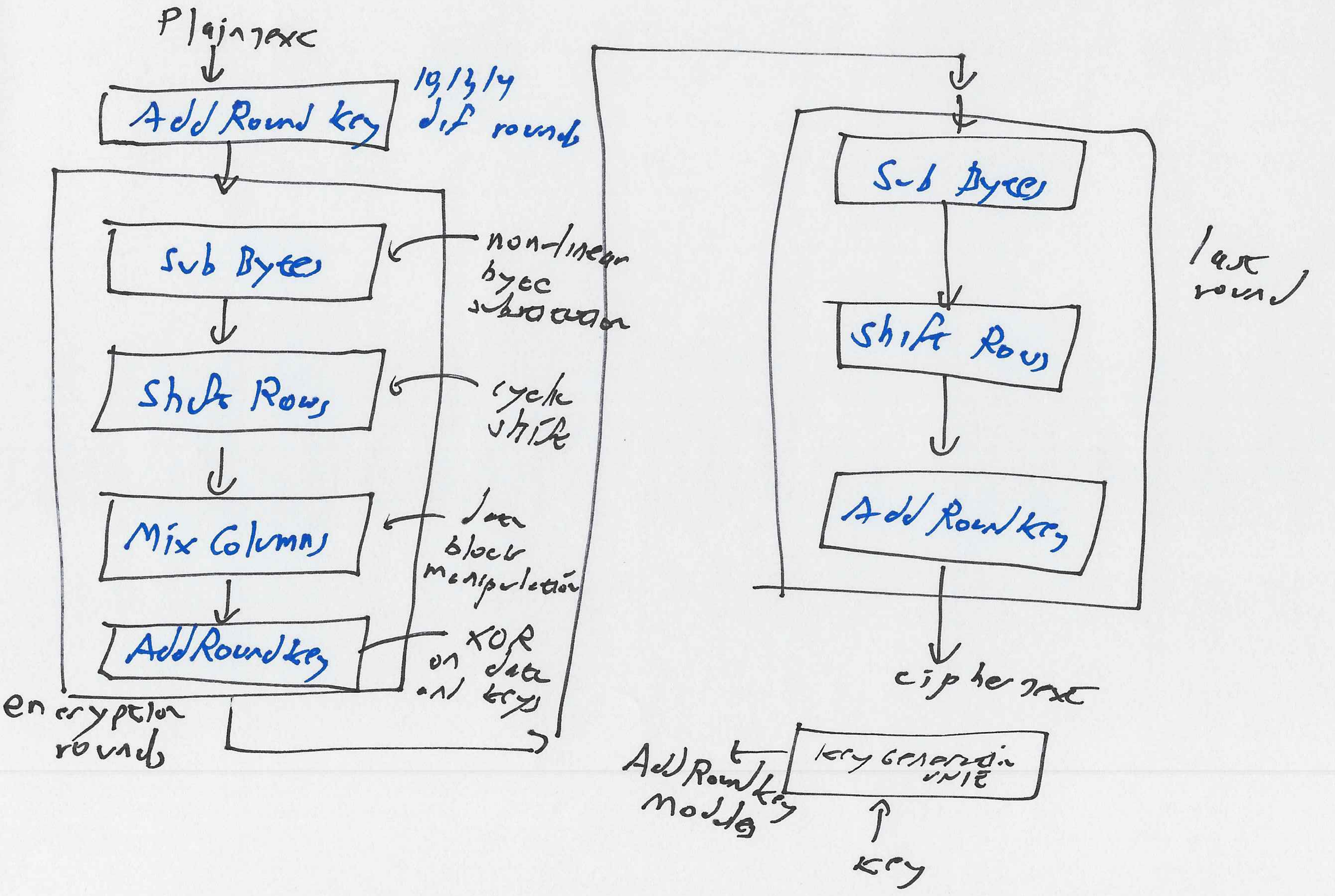
✓ Rijndael from Joan Daemen and Vincent Rijmen (Belgium)

✓ Serpent (UK, ISRAEL & DENMARK)

✓ Two Fish from team at US companies + academics.

Selected in 2000. Most popular in polls at conferences.
Since it was non-US, it smoothed acceptance.
Made official AES in DEC 2001.

AES Algorithm



AES Issues

Security – 256 bit key thought to give protection for several centuries unless breakthrough like quantum computers.

Algorithms evaluated with less rounds.

Try to find shortcuts on simpler versions.

✓ Encryption algos are different from regular products.

Not possible to differentiate between contenders on security basis.

Best attack on Rijndael worked on 7 of 10 rounds / excessive versions

- Arguments on whether simpler or complex encryption algo better.
- Rijndael went for simplicity

Performance

All contenders performed better than 3-DES.
Performance examined on RISC proc, embedded microprocessors, digital signal processing FPGA, 32 bit Pentiums, ASIC

Intellectual Property

DES patent had expired / many algorithms were patented.

Final contenders did not infringe on any patent.

Flexibility

Block ciphers like AES/DES can be used in different modes:

✓ Electronic Code Book mode

✓ Cipher Block Chaining mode : linearly chain block ciphers
so replacing a block results
in gibberish after that point.

✓ Cipher Feedback mode: byte by byte encryption.

✓ Stream Cipher Mode : continuous stream of data

Chain and feedback modes can't be parallelized.

Counter mode introduced which is parallelizable

Other modes proposed to NIST:

some are parallelizable and do
encryption, authentication & integrity protection
for just a bit more than the cost of
encryption.

However patents on these so some intellectual property issue.