Advanced Encryption Standard

Christophe Clavier

University of Limoges

AES Choice

- In January 1997 NIST made a call for candidature to define the Advanced Encryption Standard (AES)
- Indeed Data Encryption Standard DES is old and key length is not big enough, only 3-DES is considered as secure enough
- 15 candidates are proposed from different countries organisms, only 5 are selected in 1999 for final analysis: MARS, RC6, RIJNDAEL, SERPENT and TWOFISH
- RIJNDAEL is finally selected for the AES in November 2001, publication document is as U.S. FIPS PUB 197 (FIPS 197)

AES Conception

- AES has been designed by two Belgians:

Joan Daemen  Vincent Rijmen

- DES is not working on element defined in a particular mathematical field
- AES is processing on elements of the Galois Field $GF(2^8)$
- Is it not based on the Feistel Scheme, it is a Substitution Permutation Network (SPN)

AES

Three modes in AES are available for different security levels:

- AES 128 with 10 rounds: input message 128 bit, key is 128 bits long
- AES 192 with 12 rounds: input message 128 bit, key is 192 bits long
- AES 256 with 14 rounds: input message 128 bit, key is 256 bits long

AES Data Elements and $GF(2^8)$

- AES data are composed of elements of $GF(2^8)$: each byte is an element of $GF(2^8)$
- Mathematical structure gives many implementation possibilities
- Very useful also to implement protections and countermeasures against side channel attacks

Addition in $GF(2^8)$

- Each byte value is represented by a polynomial (of degree at most 7) over $GF(2) = \{0, 1\}$
- Addition over $GF(2^8)$ is simply the addition of polynomials (with coefficients in $GF(2)$)

Example

- $a(x) = x^6 + x^3 + x^2 + 1 \quad \rightarrow \quad a = 01001101_2 = 4D_{16} = 77$
- $b(x) = x^7 + x^6 + x^5 + 1 \quad \rightarrow \quad b = 11100001_2 = E1_{16} = 225$
- $c(x) = a(x) + b(x) = x^7 + x^5 + x^3 + x^2 \rightarrow c = 10101100_2 = AC_{16} = 172$

$$c = a \oplus b$$

Multiplication in $GF(2^8)$

- Multiplying two polynomials $a(x)$ and $b(x)$ may result in a polynomial of degree larger than 7
- The product is reduced modulo an irreducible polynomial $m(x)$ of degree 8 (for AES, $m(x) = x^8 + x^4 + x^3 + x + 1$ $(11B_{16})$)

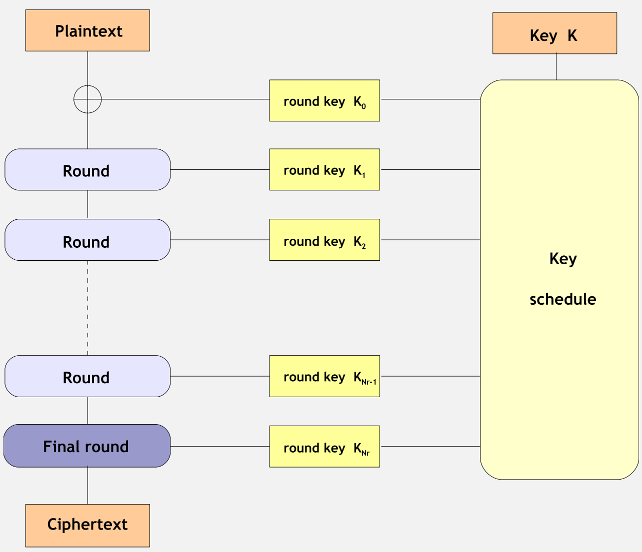
Example

- $a(x) = x^6 + x^3 + x^2 + 1 \quad \to \quad a = 01001101_2 = 4D_{16} = 77$
- $b(x) = x^7 + x^6 + x^5 + 1 \quad \to \quad b = 11100001_2 = E1_{16} = 225$
- $a(x) \cdot b(x) = x^{13} + x^{12} + x^{11} + x^{10} + x^5 + x^3 + x^2 + 1$
- $c(x) = a(x) \cdot b(x) \bmod m(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \to c = 7F_{16}$

$$4D \cdot E1 = 7F$$

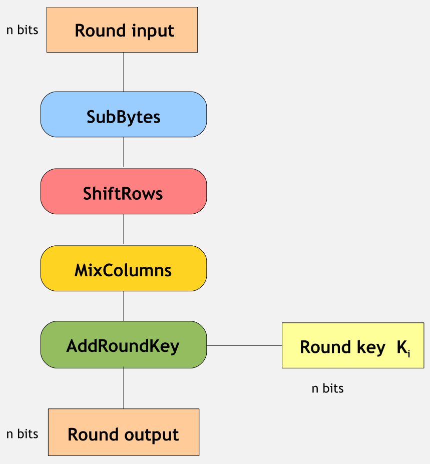
Université de Limoges

The whole AES



Université de Limoges

One AES round



AES round

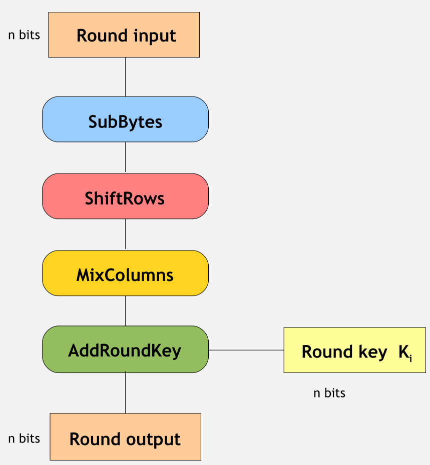
SubBytes Non-linear substitution on bytes (S-Box)

ShiftRows Row-wise byte permutation

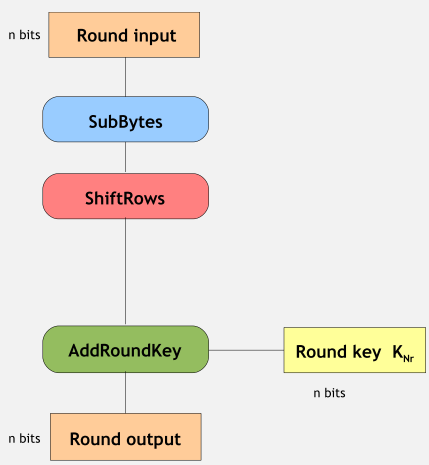
MixColumns Colums are multiplied by a circulant matrix

AddRoundKey Addition of bytes in $GF(2^8)$ (XOR with K_i)

A particular final round



Normal round



Final round

Cryptnalysis

- AES has been designed to resist to differential cryptanalysis
- AES has been designed to resist to linear cryptanalysis
- No known/chosen plaintext attack is known on any of AES-128, AES-192 and AES-256
- A chosen plaintext attack on reduced round variants can break:
  - 7 rounds of 128-bit AES
  - 8 rounds of 192-bit AES
  - 8 rounds of 256-bit AES
- In 2009, related key attacks have been discovered on full 192-bit and 256-bit AES (not practical as requiring 2^{176} and 2^{119} encryptions respectively)

Conclusion

- AES is still today considered as a secure algorithm
- "Algebraic structure gives opportunities for discovering an attack on AES" can be heard... but nothing yet...
- Other final candidates MARS, RC6, SERPENT and TWOFISH are also recommended by NIST as secure algorithms