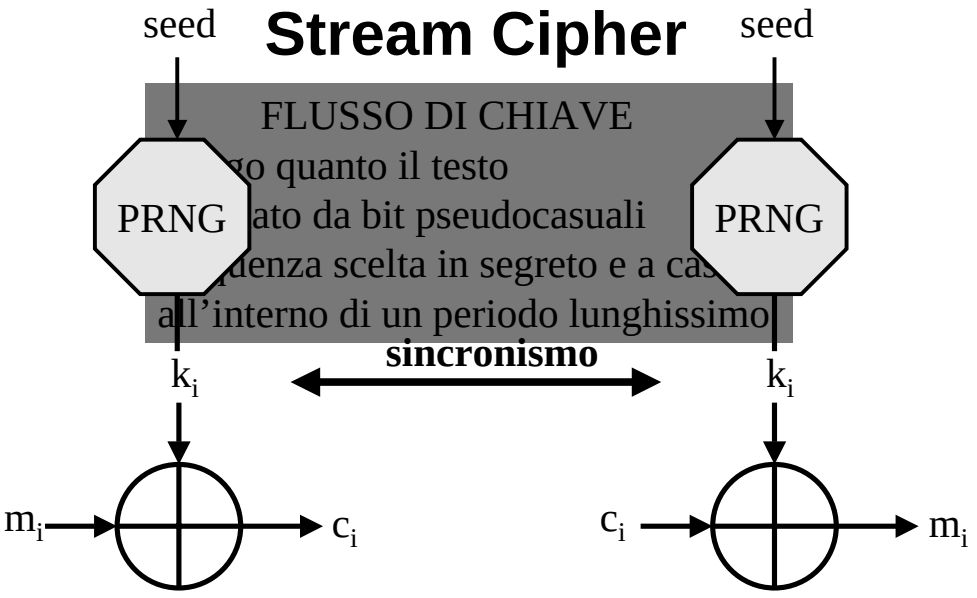
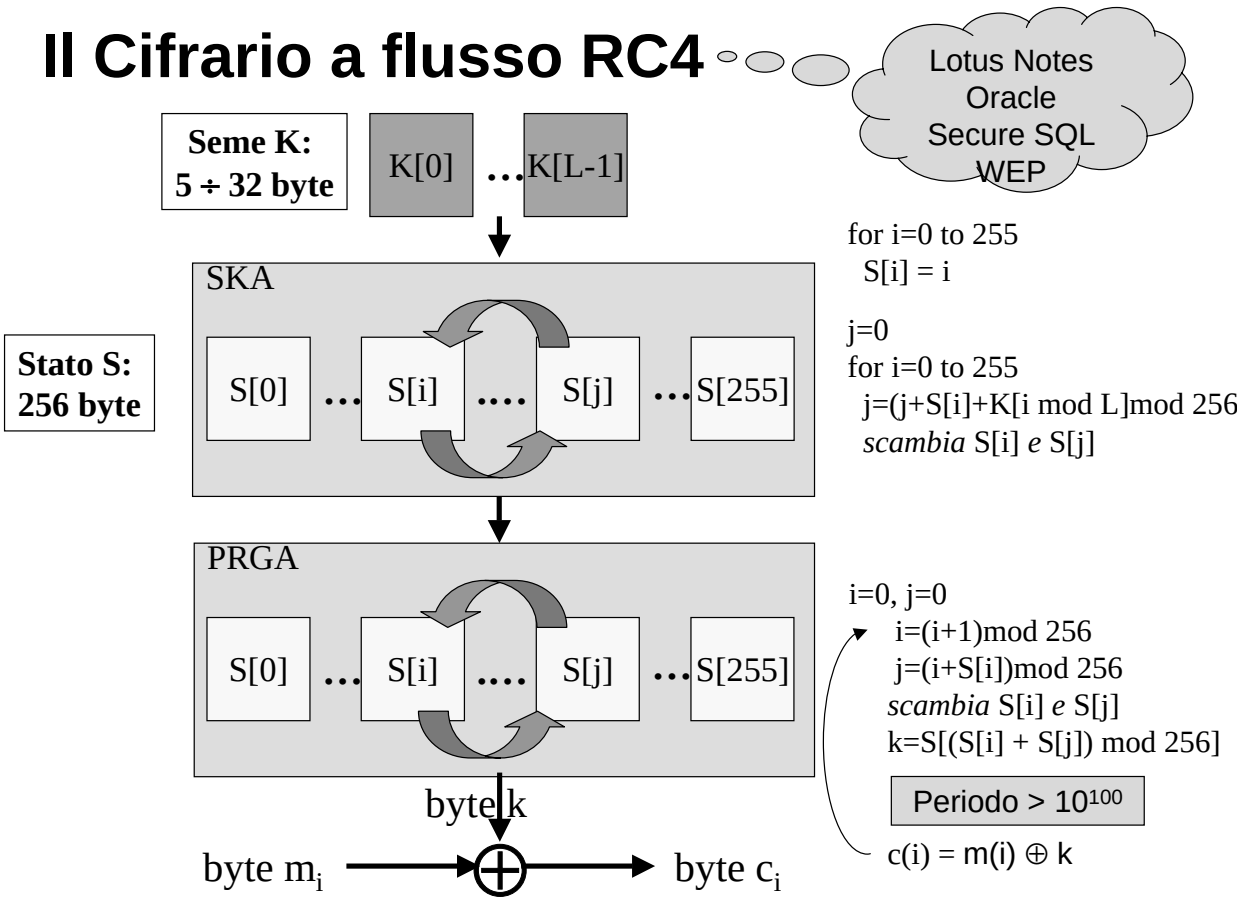
Stream Cipher



CIFRATURA
$c_i = m_i \oplus k_i$
i= 1, 2, 3, ..

DECIFRAZIONE
$c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$
$= m_i$
i= 1, 2, 3, ..

Il Cifrario a flusso RC4



for i=0 to 255
S[i] = i

j=0
for i=0 to 255
j=(j+S[i]+K[i mod L]mod 256
scambia S[i] *e* S[j]

i=0, j=0
i=(i+1)mod 256
j=(i+S[i])mod 256
scambia S[i] *e* S[j]
k=S[(S[i] + S[j]) mod 256]

Periodo > 10^{100}

c(i) = m(i) ⊕ k

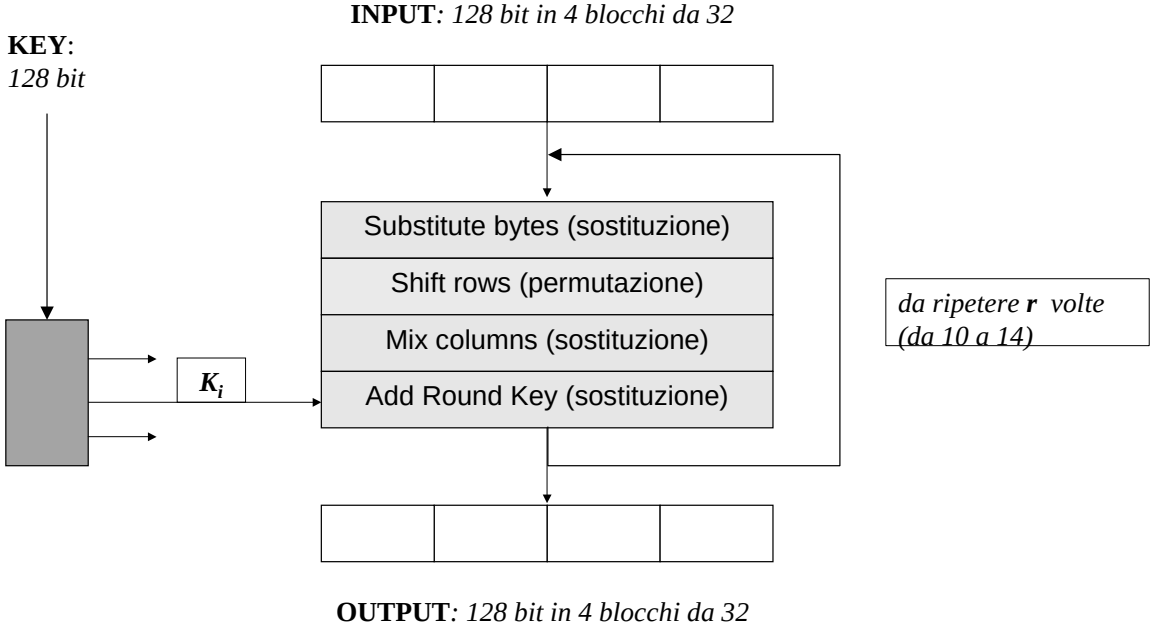
Advanced Encryption Standard

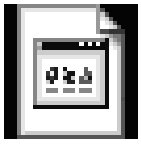
5 finalisti su 16 candidati:
MARS, RC6, Rijndael, Serpent, Twofish

Valutazione di Rijndael

- eccellenti prestazioni su tutte le piattaforme (dai main frame alle smart card),
- buon margine di sicurezza a fronte di ogni attacco conosciuto,
- bassa richiesta di memoria, sia ROM che RAM,
- veloce procedura di key setup,
- buone caratteristiche per l'esecuzione parallela delle istruzioni,
- chiavi e blocchi di lunghezza variabile per multipli di 32 bit.

Un round di Rijndael





Rijndael_ingles_2004.exe