VERNAM CIPHER

CESAR CIPHER

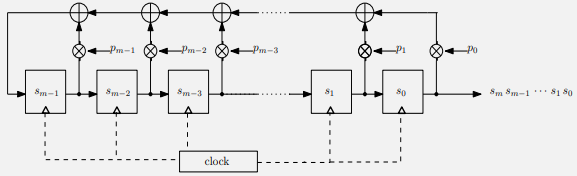
CIRULAR SHIFT CIPHER

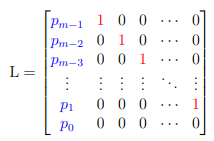
Lehmer generator and LCG



Fibonacci LFSR



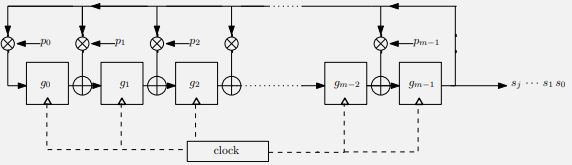
 

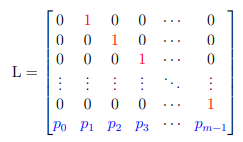






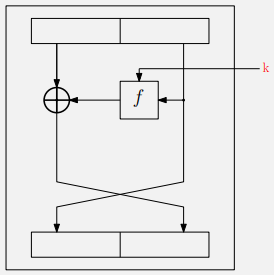
Galois LFSR





FEISTEL ROUND



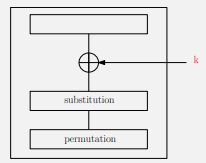
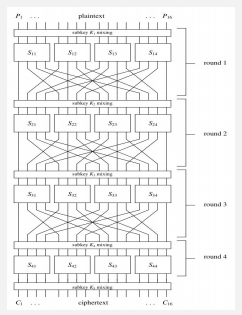
**B**

**B**

**A**

**A**

SOBSTITUTION-PERMUTATION NETWORK

CBC CIPHERING



CBC DECIPHERING



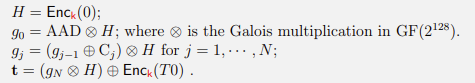
CTR CIPHERING



CTR DECIPHERING



GCM tag t



Euler’s Criterion



Euler’s FUNCTION

, , , 



FERMAT’S LITTLE THEOREM



CRT

, , ,

f(a,b) = a\*f(1,0) + b\*f(0,1)

HMAC

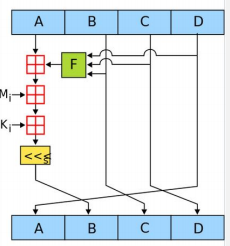
Immagine che contiene testo

Descrizione generata automaticamente

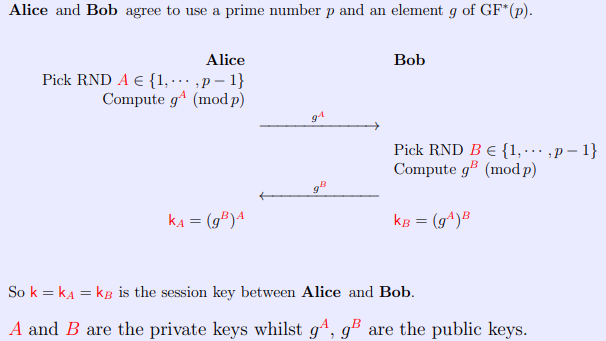


David-Meyer function Com

MD4 COMPRESSION



DIFFIE-HELMAN



ELGAMAL

Immagine che contiene testo

Descrizione generata automaticamente

RABIN TEXTBOOK

Immagine che contiene testo

Descrizione generata automaticamente

RSA TEXTBOOK

Immagine che contiene testo

Descrizione generata automaticamente

NAÏVE RSA-SIGNATURE

Immagine che contiene testo

Descrizione generata automaticamente

DSA – GEN

Immagine che contiene testo

Descrizione generata automaticamente

DSA -SIGN

Immagine che contiene testo

Descrizione generata automaticamente

DSA – VERIFY

Immagine che contiene testo

Descrizione generata automaticamente

POINT ADDITION



 Immagine che contiene testo

Descrizione generata automaticamente

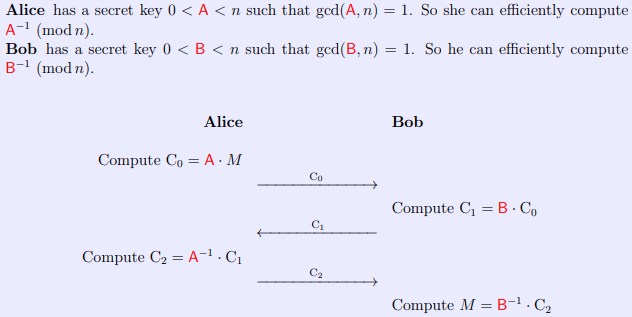
POINT DOUBLING



EC– HD Immagine che contiene testo

Descrizione generata automaticamente

EC – MASSEY-OMURA



EC – DSA GEN

Immagine che contiene testo

Descrizione generata automaticamente

EC – DSA SIGN

Immagine che contiene testo

Descrizione generata automaticamente

EC – DSA VERIFY

Immagine che contiene testo

Descrizione generata automaticamente