Criptografia FIB

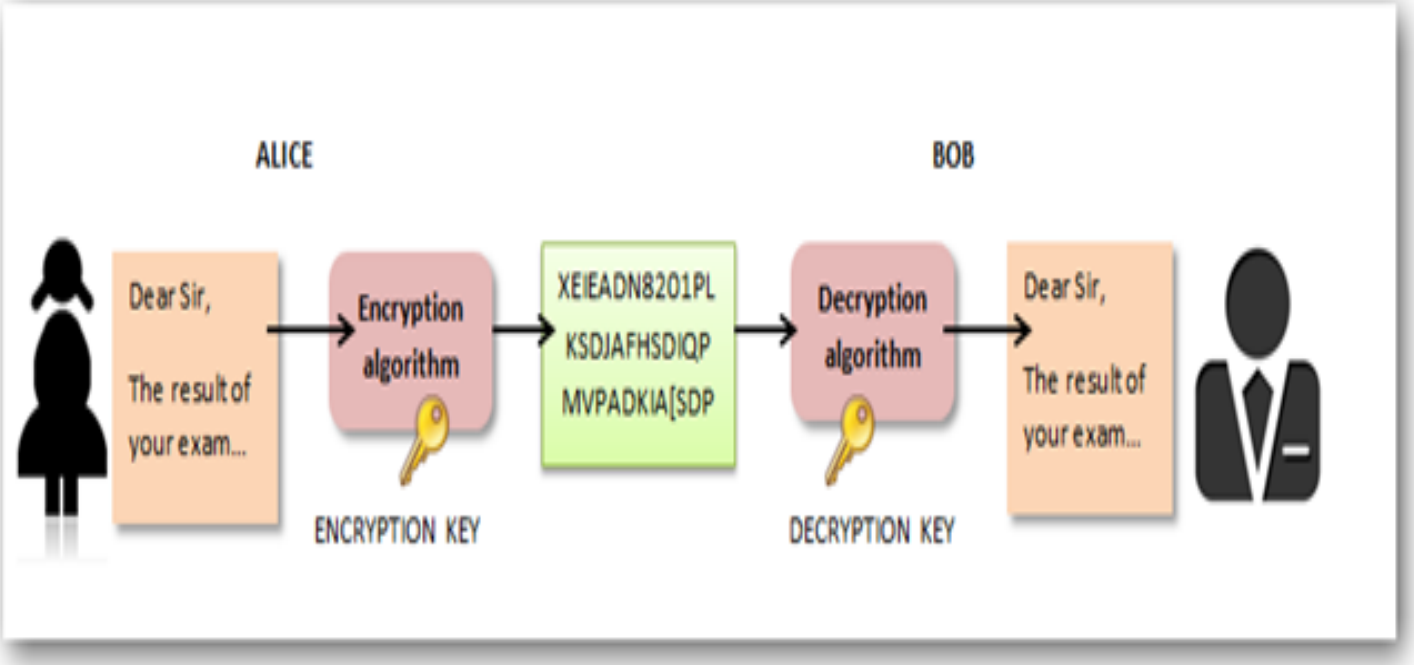
Criptografia de clau secreta

Anna Rio

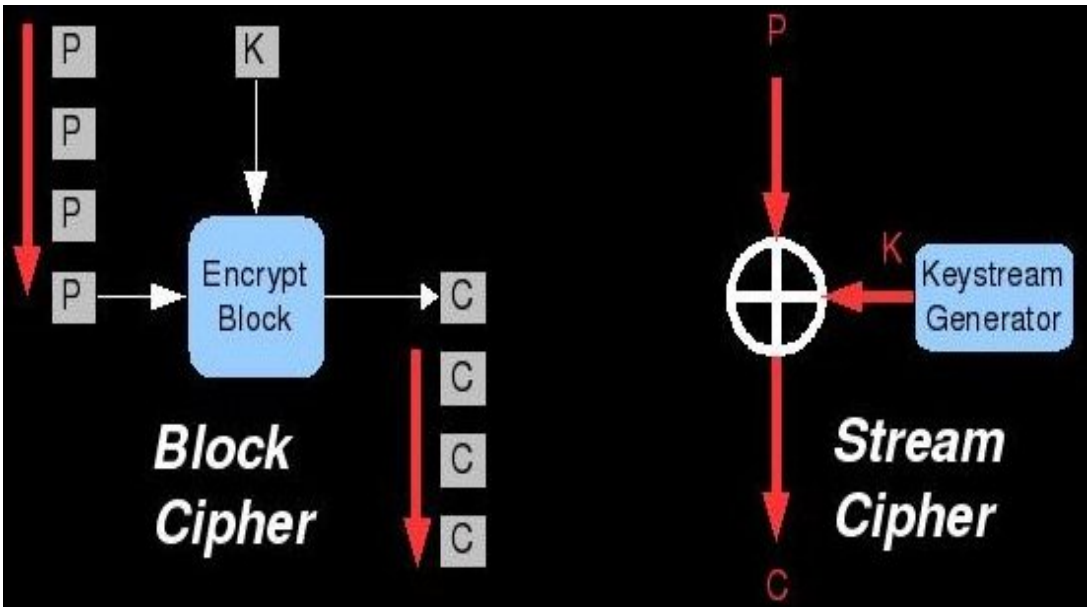
Departament de Matemàtica Aplicada II • Universitat Politècnica de Catalunya

Criptografia de clau secreta

Mètodes simètrics: s'utilitza la mateixa clau per xifrar i desxifrar



Criptografia de clau secreta: dos mètodes (Bulk Ciphers)



Criptografia de clau secreta: dos mètodes

Xifratge en flux

El missatge es processa bit a bit
RC4

Són més ràpids i tenen menys complexitat de hardware. Seguretat?

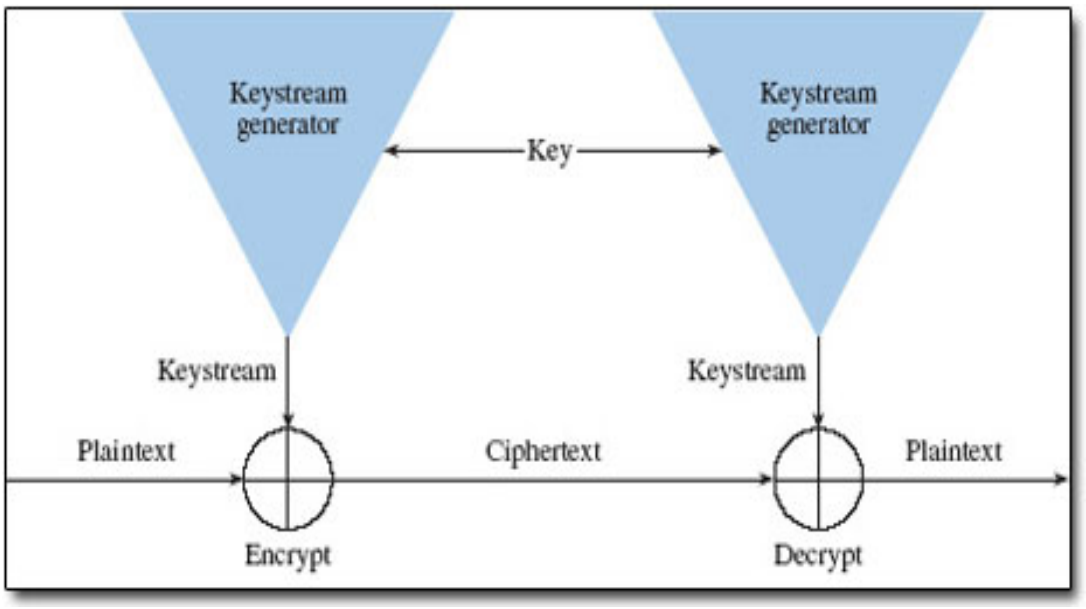
Xifratge en bloc

El missatge es divideix en blocs de la mateixa longitud als quals s'aplica la mateixa transformació de xifratge
DES, IDEA, RC5, AES

NIST Standards

Xifratge en flux

Emissor i receptor acorden una clau (curta) i un algoritme (determinístic) generador de seqüència xifrant (cadena de bits pseudoaleatòria)

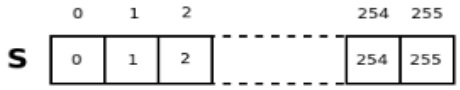


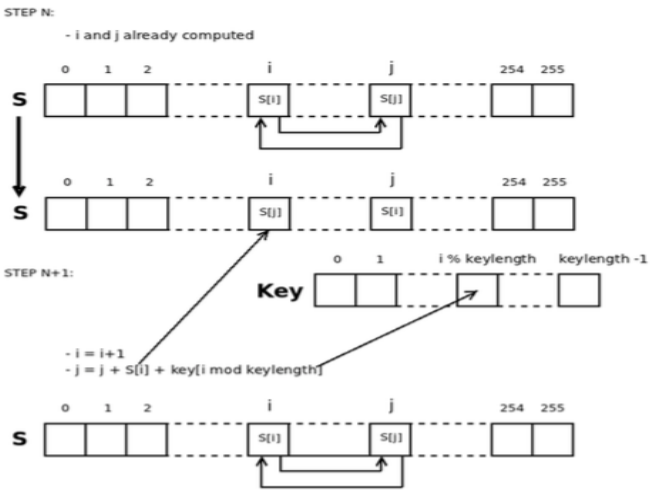
Generadors binaris pseudoaleatoris

- Període $> 10^{38}$ (superior a la longitud de qualsevol text a xifrar)
- Distribució uniforme de zeros i uns
  Postulats de Golomb:
  1. Mateix nombre de zeros i uns
  2. Digrames $00, 01, 10, 11$ equirepartits,
     trigrames, $\ldots$, $n-$grames
  3. Les coincidències entre la seqüència i la seva desplaçada no proporcionen informació sobre el període
- Imprevisibilitat: donada una porció, no es pot predir el següent dígit amb probabilitat d'encert superior a 1/2
- Facilitat d'implementació

RC4

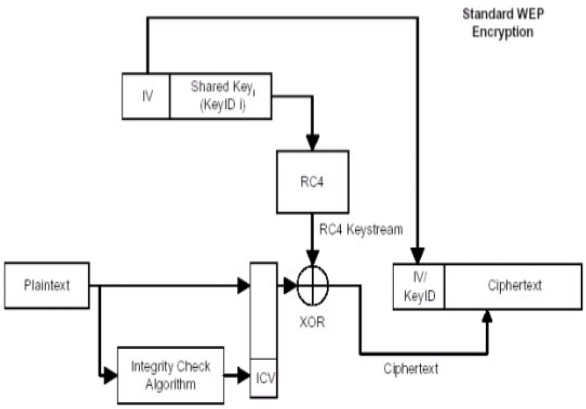
- Dissenyat per Rivest per a RSA Security (**R**ivest **C**ipher o **R**on's **C**ode)
- Claus de fins a 2048 bits
- Període probablement més gran que 10^{100}





RC4: WEP

Wired Equivalent Privacy (WEP) algoritme de seguretat per a les xarxes wireless IEEE 802.11

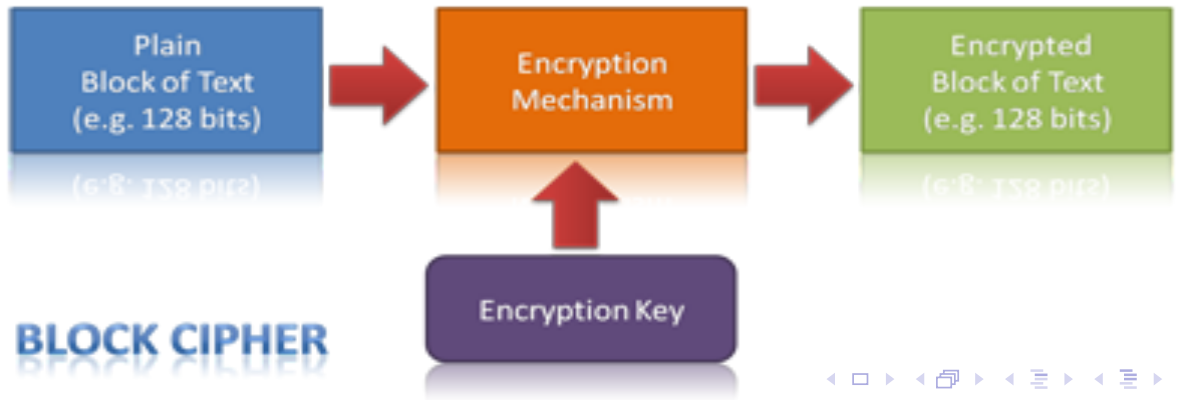


Per a un IV de 24 bits, probabilitat del 50% de repetició del IV després de 5000 execucions. Declarat obsolet el 2004

Xifratge en bloc: propietats

L'entrada de l'algoritme és un bloc de bits de longitud fixada (múltiple de 64)

- cada símbol es xifra de manera dependent dels adjacents
- cada bloc es xifra sempre d'igual manera, independentment de la seva posició en el missatge
- un missatge es pot desxifrar parcialment, a partir del bloc que interessi



Xifratge en bloc: Arquitectura

Transformació inicial Introdueix aleatorietat

Funció iterada r vegades ("tombs") Funció no lineal (complicada) de les dades i la clau, que pot definir-se mitjançant diverses transformacions simples. Els tombs es connecten amb un XOR bit a bit

Transformació final. Simetritza xifratge i desxifratge

Algoritme d'expansió de clau. La clau de l'usuari (curta) es transforma en un conjunt de subclaus (molts bits)