



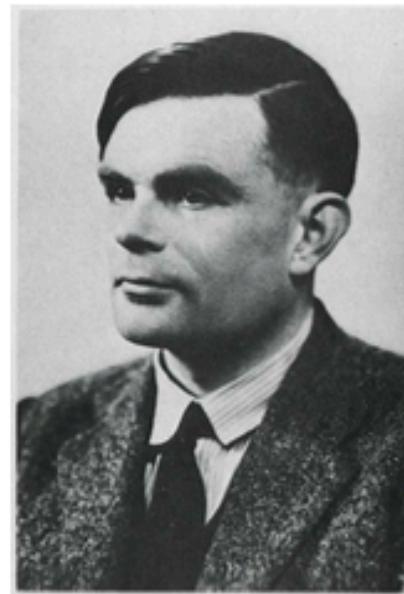
Criptografia

Anna Rio • FIB • 2015



ORIGENS DE LA CRIPTOGRAFIA MODERNA

- 1938 El govern britànic instal.la a **Bletchley Park** la *Foreign Office's Code and Cipher School*
- 1940 S'incorpora **Alan Mathison Turing** (1912-1954). Durant la 2a Guerra Mundial, deu mil persones hi treballen. El repte per a matemàtics i criptoanalistes és trencar el criptosistema **Enigma**, que utilitzava l'exèrcit alemany



ORIGENS DE LA CRIPTOGRAFIA MODERNA

1944 Es posa en funcionament **Colossus**, la primera computadora electrònica programable.



D'UN ART ANTIC A UNA NOVA CIÈNCIA

Fins a la 2a. Guerra Mundial, la Criptografia era un art, principalment d'ús en àmbits militars, concentrat quasi exclusivament en el xifratge, que usava sistemes ad-hoc sense base teòrica de la seva seguretat

Transició cap a la nova ciència

- 1948 C. E. **Shannon**: *A mathematical theory of communication*
Bell System Technical Journal
- 1949 C. E. **Shannon**: *Communication theory of secrecy systems*
Bell System Technical Journal
- 1976 W. **Diffie** i M. E. **Hellman**: *New directions in cryptography*
IEEE Transactions on Information Theory

XIFRAT DE VERNAM (1917)



Gilbert Sandford Vernam (1890–1960)



CINJT UUHML FRUGC ZIBGD BOPNI PDNJG LPLLP YJYXM
DCKAC JSJUK BIOYT HWQFX DLIRC BEXYK VKIMB TYIPE
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI
DZJYO YKAIE LIUYW DFOHU IOHZV SRNDD KPSSO JHPQT
MHQHL OHQOD SMHONP HHOHQ GXRPJ XBXIP LLZAA VCMOG
AWSSZ YMFMN ATMION IXFBY FOZLE CVYSJ XZGPU CTFQY
HOVHU OCJGU QMWQV OIGOR BPHIZ TYPDB VBRMN XNLZC

One Time Pad

missatge	00011 01111 01101 00101
⊕	
clau	11011 00101 01011 00110
↓	
criptograma	11000 01010 00110 00011
⊕	
clau	11011 00101 01011 00110
↓	
missatge	00011 01111 01101 00101

XIFRAT DE VERNAM (1917)

Proposat per a transmissions telegràfiques

Utilitza un alfabet de 32 símbols representats per 5 bits

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^* = \mathbf{F}_2^*$$

$$E(x, k) = D(x, k) = x + k$$

La **clau** és una seqüència binària aleatòria de la mateixa longitud que el missatge i no reutilitzable

Xifra i desxifra amb **XOR** bit a bit

És l'únic sistema **incondicionalment segur** coneugut

SEGURETAT D'UN CRIPTOSISTEMA

Incondicionalment segur

La probabilitat que un criptograma provingui d'un missatge determinat és igual que la probabilitat a priori d'aquest missatge

$$\text{Prob}(M = m / C = c) = \text{Prob}(M = m)$$

Dit d'una altra manera, el criptograma no aporta cap informació sobre el missatge. ([Teoria de Shannon](#))

Computacionalment segur

Amb recursos de càlcul limitats no es pot trencar.

SHANNON: TEORIA DE LA INFORMACIÓ

1948: A Mathematical Theory of Communication

Llenguatge: procés estocàstic que proporciona cadenes de símbols de l'alfabet

Quantitat d'informació d'una cadena de símbols:

$$\text{Inf}(m) = -\log(\text{prob}(m)) \text{bits}$$

Entropia d'una cadena de símbols: $H(m) = \text{prob}(m)\text{Inf}(m)$

Entropia d'una font d'informació: valor mitjà ponderat de la qüantitat d'informació dels diferents estats.

$$H(S) = \sum \text{prob}(m_i)\text{Inf}(m_i)$$

Exemple: Un alfabet de 27 símbols equiprobables té entropia 4,75 bits/símbol

SHANNON: SECRET PERFECTE



Claude Elwood Shannon (1916–2001)

1949: Communication Theory of Secrecy Systems

Hipòtesi: clau d'un sol ús i el criptoanalista només té accès al criptograma.

Definició: Un sistema criptogràfic és perfectament segur si el text clar és estadísticament independent del criptograma:

$$\text{Prob}(M = m / C = c) = \text{Prob}(M = m)$$

És a dir, la informació sobre el missatge aportada pel criptograma és nul.la. (Independentment del temps i recursos computacionals emprats)

TEOREMES DE SHANNON

Basant-se en el concepte d'entropia, Shannon demostra:

- ① És condició necessària que la longitud de la clau sigui més gran o igual que la del missatge
- ② Existeixen sistemes perfectament segurs, en concret, el xifrat de Vernam ho és

- En el panorama criptogràfic actual el xifrat de Vernam és l'únic sistema incondicionalment segur que es coneix.
- És el sistema utilitzat en la [hotline](#) entre la Casa Blanca i el Kremlin que es va establir el 30 d'agost de 1963 i que es manté en funcionament.
- Les claus són transferides **a mà**, en presència de testimonis i en condicions de màxima seguretat

CRIPTOGRAFIA QUÀNTICA

Quantum key distribution

Utilitzar els principis de la mecànica quàntica, com ara el principi d'incertesa de Heisenberg o l'entrellaçament quàntic, per fer un sistema d'intercanvi de claus totalment segur

Si s'espia la transmissió, aleshores es modifica.. **La incertesa del món quàntic proporciona certesa sobre la seguretat de les comunicacions**

BB84 Protocol de distribució quàntica de claus basat en la transmissió de fotons a través d'un canal quàntic

2012 "Quantum teleportation over 143 kilometres using active feed-forward". *Nature*. 489 (7415): 269–273.

2015 Researchers at the National Institute of Standards and Technology (NIST) have "teleported" or transferred quantum information carried in light particles over 100 kilometers of optical fiber, four times farther than the previous record

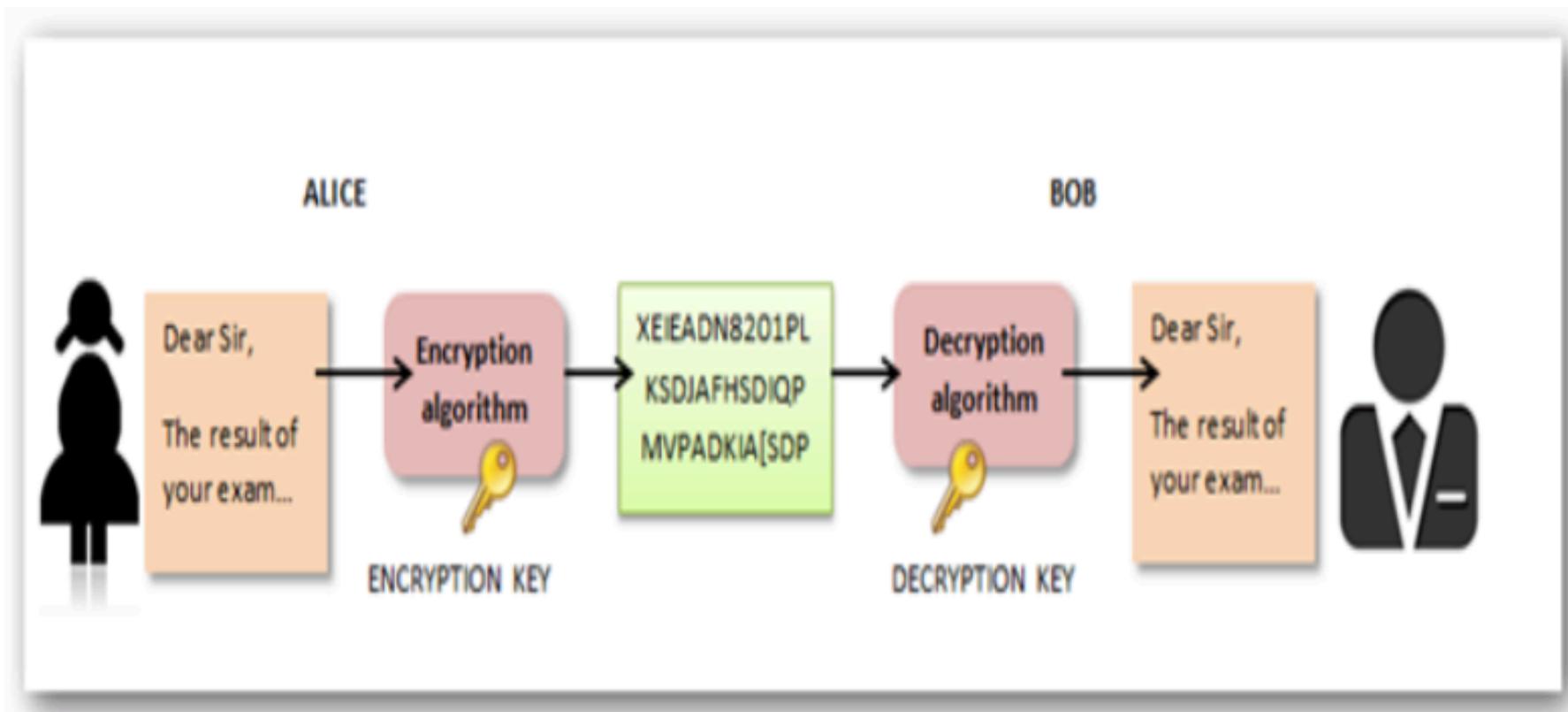
2015 Researchers in the US have set a new quantum record, using photons to carry messages between two electrons almost 2 km (1.2 miles) apart

CRIPTOGRAFIA MODERNA

- **Problema n^2** En una xarxa de n usuaris hi ha $O(n^2)$ parelles.
Sistema criptogràfic comú, **cada parella una clau secreta diferent.**
Calen criptosistemes dissenyats per a ser compartits per un gran nombre d'usuaris, que depenguin d'una clau secreta fàcil de construir
- **Príncipi de Kerchoff** Sistema dissenyat per algú altre, comercialitzat per algú altre, sota les lleis d'un altre país, implementat en n punts d'una xarxa....
La seguretat no pot dependre de mantenir en secret el sistema criptogràfic
- **Llei de Moore** Si el sistema pretén mantenir secrets a llarg termini, la longitud de la clau s'ha de triar resistent a la cerca exhaustiva amb les **capacitats computacionals futures**
- **Llei de Murphy** Si hi ha un forat, per petit que sigui, en la seguretat, algú el trobarà i algú acabarà fent-ne un mal ús. La seguretat no s'acumula: **un sistema és tan segur com ho sigui la seva part més feble**

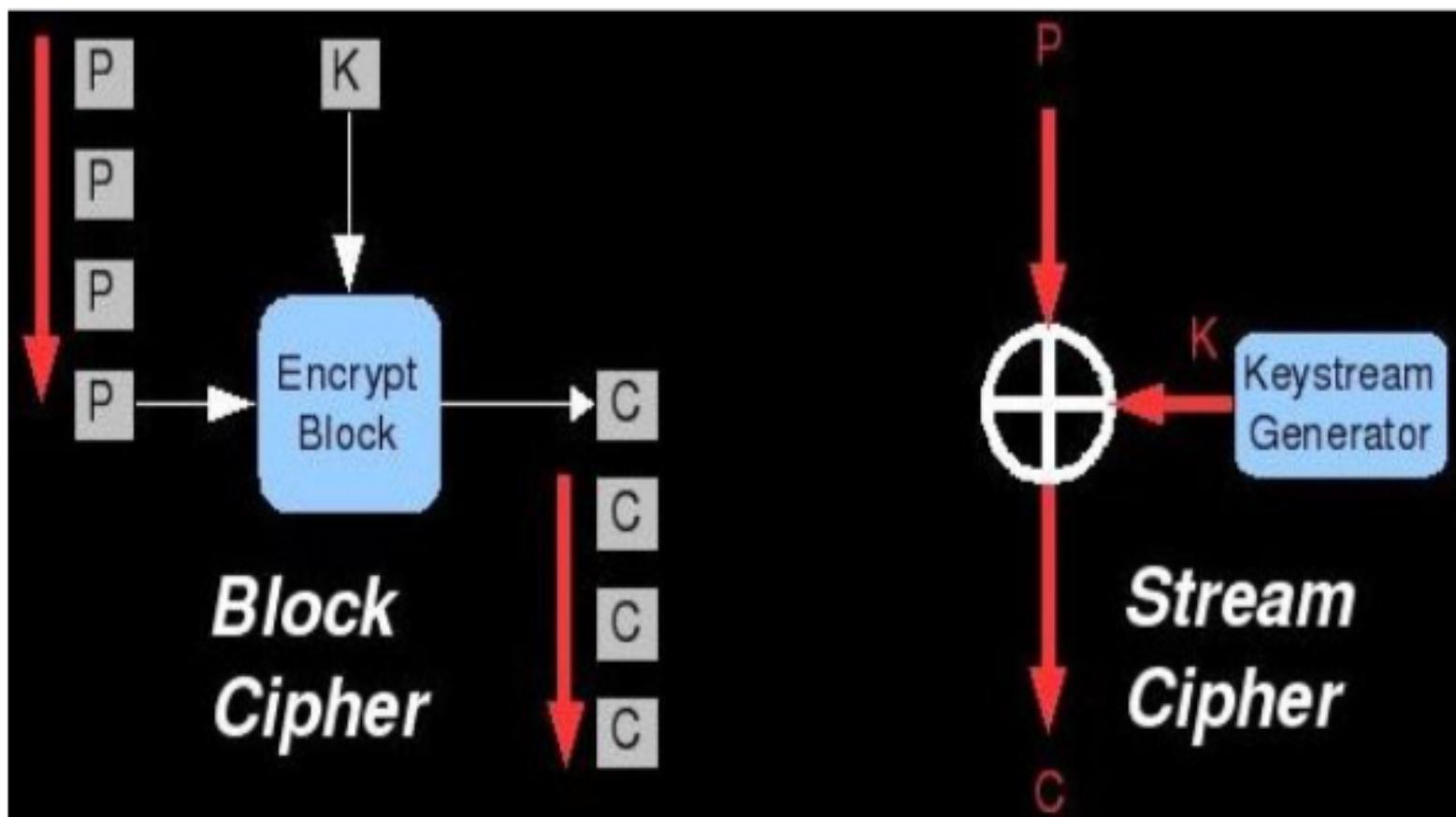
CRIPTOGRAFIA DE CLAU SECRETA

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



CRIPTOGRAFIA DE CLAU SECRETA

Dos mètodes



CRIPTOGRAFIA DE CLAU SECRETA

Xifratge en flux

El missatge es processa bit a bit

RC4

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

Xifratge en bloc

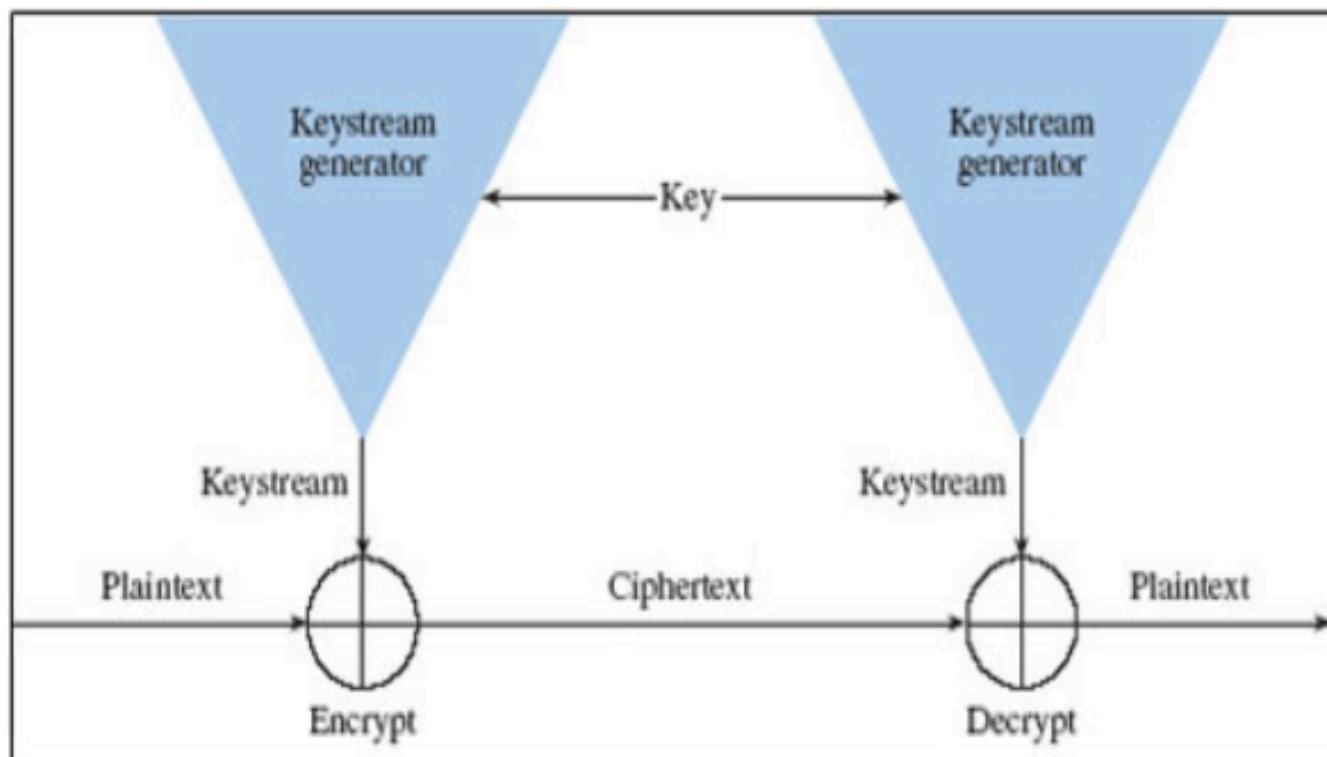
El missatge es divideix en blocs de la mateixa longitud als quals s'aplica la mateixa transformació de xifratge

DES, IDEA, RC5, AES

NIST Standards

XIFRATGE EN FLUX (STREAM CIPHERS)

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

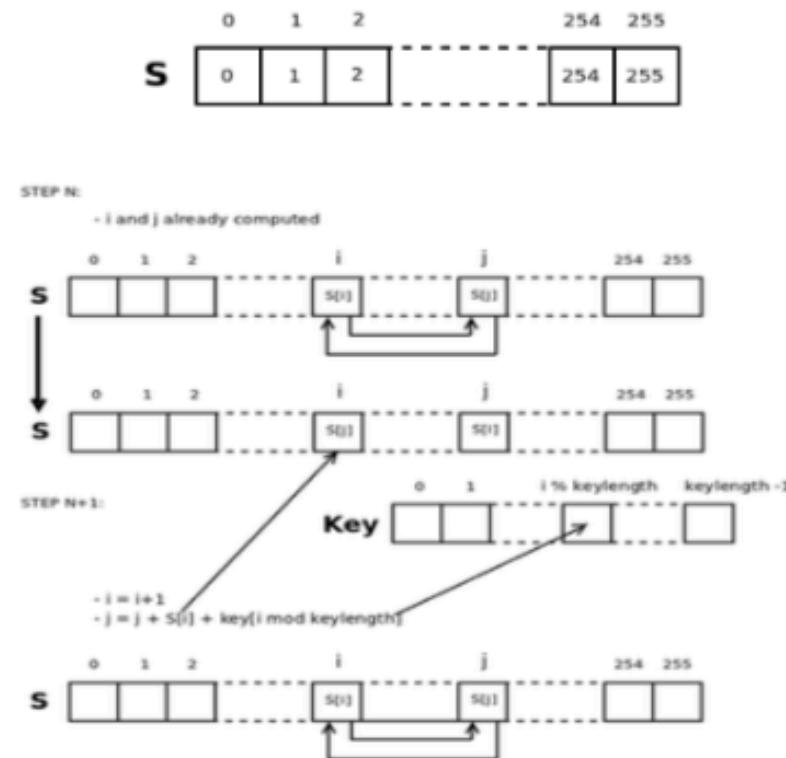


GENERADORS BINARIS PSEUDOALEATORIS

- 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, ..., 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

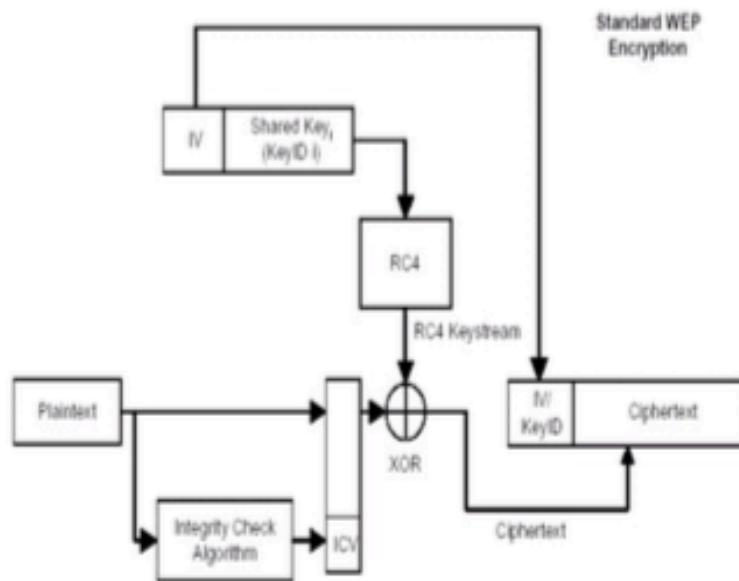
RC4

- Dissenyat per Rivest per a RSA Security (**Rivest Cipher o Ron's Code**)
- 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

