

Crittosistemi simmetrici moderni

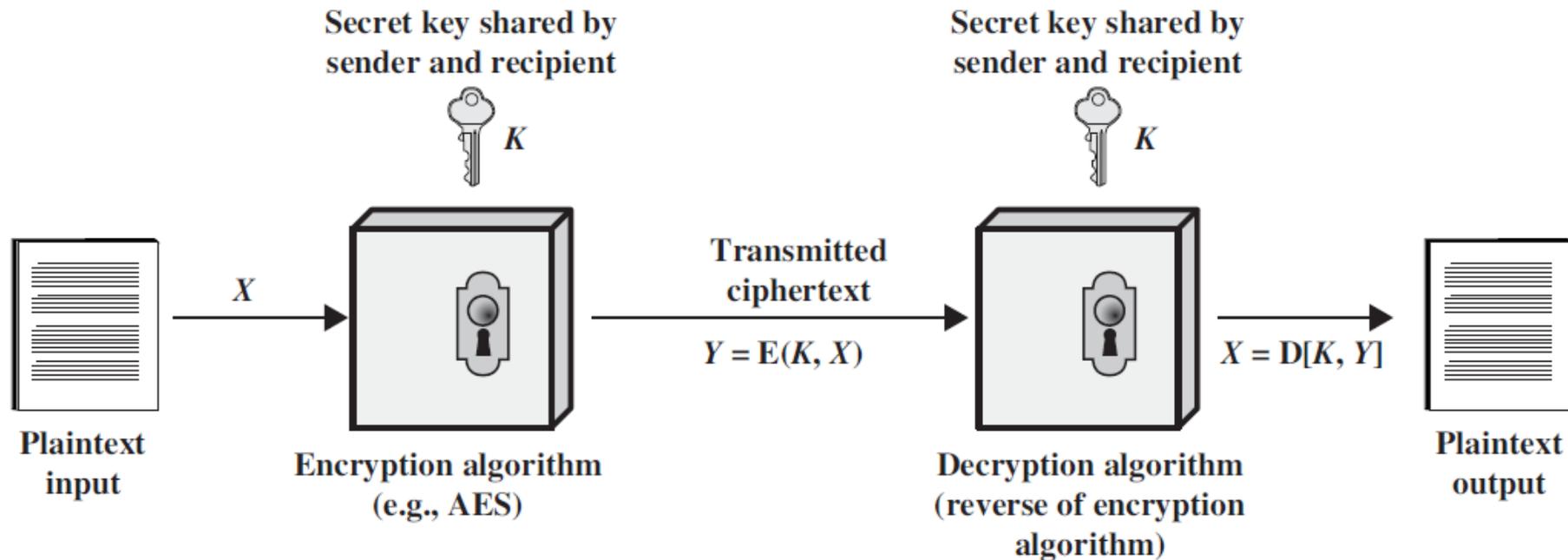
Cifrari a blocco

- In molti sistemi crittografici precedenti, la modifica di una lettera nel del testo in chiaro cambia esattamente una lettera nel testo cifrato.
- In questo modo gli attacchi basati sull'analisi delle frequenze sono molto semplici.
- I cifrari a blocchi possono evitare questi problemi criptando simultaneamente blocchi di molte lettere o numeri.

Cifrari simmetrici contemporanei

Name	Block Size / Key Size (bits)¹	Description
AES [5]	128 / 128	US Federal standard for block encryption since 2001.
DES 3DES [6]	64 / 56 64 / 112	Former standards for block encryption.
IDEA, Blowfish [6]	64 / 128	Used in OpenSSL, WTLS, GPG and SSH.
RC4 ² [6]	8 / 128	Used in WEP - part of the WLAN standard IEEE 802.11 [8].
RC5 [6]	64 / 128	Used in the WTLS security protocol specified in WAP [9].
RC6, MARS, Twofish, Serpent	128 / 128	AES finalists [10].

Algoritmi a chiave simmetrica



- Esempi:
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)

Esperimento online

- <https://cryptii.com/>

The screenshot displays the Cryptii online encryption tool interface. It is divided into three main sections: Text, Block Cipher, and Bytes.

Text Section: The input text is "The quick brown fox jumps over the lazy dog."

Block Cipher Section: The settings are as follows:

- ALGORITHM: AES-128
- MODE: CBC (Cipher Block Chaining)
- KEY: 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 c
- IV: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c

The output is "→ Encoded 48 bytes".

Bytes Section: The output is displayed in Hexadecimal format, grouped by Byte. The resulting hex string is: bd 13 20 4f 67 d8 16 7f 20 21 1c 99 b0 a7 cc 05 06 d5 c7 03 ea fb 01 a7 d0 47 3b 5c c9 99 aa a2 1e 01 7b 76 6e 52 98 5f 5e f7 f0 bd c5 72 b7 2e.

Diffusione

- Ogni buon crittosistema dovrebbe avere questa proprietà per prevenire gli attacchi basati sull'analisi statistica [Shannon]
- Si ha diffusione quando la modifica di **un carattere del testo in chiaro** fa cambiare **molti caratteri del testo cifrato** e, analogamente, la modifica di **un** carattere del testo cifrato fa cambiare **molti** caratteri del testo in chiaro
- Le statistiche di lettere, digrafi, trigrafi, ecc. sono **diffuse** su molti caratteri del testo cifrato e questo rende più difficili gli attacchi statistici

Confusione

- Ogni buon crittosistema dovrebbe avere questa proprietà per prevenire gli attacchi basati sull'analisi statistica [Shannon].
- Si ha confusione quando la chiave segreta non è collegata al testo cifrato in modo semplice.
- In particolare, ogni carattere del testo cifrato deve dipendere da molte parti della chiave (eventualmente dall'intera chiave).

Confusione

- I cifrari a sostituzione non possiedono le proprietà di diffusione e confusione, e questo è il motivo per cui sono vulnerabili all'analisi delle frequenze
- Dal punto di vista di Bob, uno svantaggio della confusione è la propagazione degli errori: pochi errori nel testo cifrato danno origine a molti errori nel testo in chiaro, rendendolo incomprensibile