CIFRARI A BLOCCHI

16/03/2023

Nelle leziomi precedenti abbiamo studiato DES e AES: due esempi di CIFRARI A BLOCCHI.

I cifrari infatti possono essere di due tipi:

- **CIFRARI A BLOCCHI** (Block Cipher)
- **CIFRARI A FLUSSO** (Stream Cipher)

Im questa ottica, nascono due problemi:

- usare CHIAVI PIU` LUNGHE ← problema comune ad entrambi i cifrari

Il grafico seguente, ci fa visualizzare concretamente come la lunghezza della chiave sia un fattore cruciale per rendere difficile (se non impossibile) la vita al nostro avversario:

DES

bit	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	
gg	5	10	20	40	80	160	320	640	1280	2560	5120	10240	20480	40960	81920	163840	327680	655360	
Anni	0,01	0,03	0,05	0,11	0,22	0,44	0,88	1,75	3,51	7,01	14,03	28,05	56,11	112,22	224,44	448,88	897,75	1.795,51	
bit	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
Anni	7000	14000	28000	56000	112000	224000	448000	896000	1792000	3584000	7168000	14336000	28672000	57344000	114688000	229376000	458752000	917504000	1835008000
MILIONI di anni	0,007	0,014	0,028	0,056	0,112	0,224	0,448	0,896	1,792	3,584	7,168	14,336	28,672	57,344	114,688	229,376	458,752	917,504	1835,008
bit	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
MILIARDI Di Anr	3,67	7,34	14,68	29,36	58,72	117,44	234,88	469,76	939,52	1879,04	3758,08	7516,16	15032,32	30064,64	60129,28	120258,5	240517,1	481034,2	962068,4

- cifrare TESTI PIU` LUNGHI ← problema dei soli CIFRARI A BLOCCHI

CHIAVI PIU' LUNGHE

Concentriamoci sul 1° problema: Posso allungare la chiave utilizzando lo stesso algoritmo ?

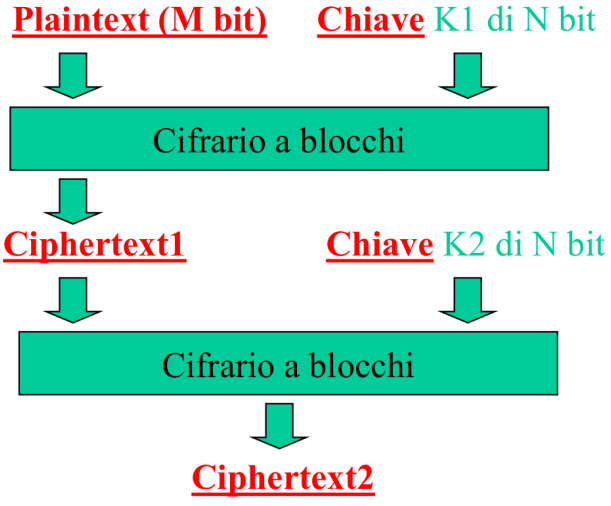
In realtà abbiamo già osservato ed affrontato questo tipo di problema:

> una chiave corta rende il CIFRARIO debole rispetto ad ATTACCHI DI FORZA BRUTA

L'idea è: **CIFRATURA A n-FASI** cifro più volte, ogni volta con una chiave diversa.

Controintuitivamente però, questo non rende sempre più forte il cifrario:

CIFRATURA A 2-FASI → NON sicuro poiché possibile ATTACCO DI FORZA BRUTA basato su Ciphertext1



Testo cifrato intermedio

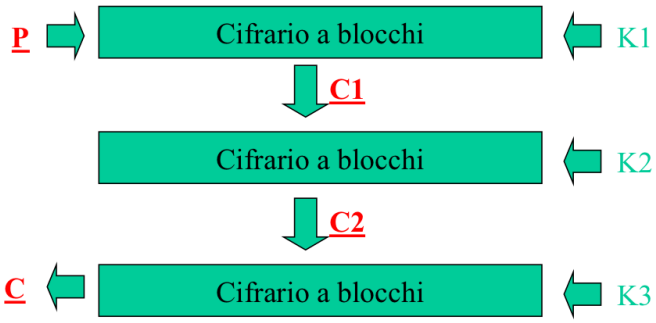
ATTACCO **MEET IN MIDDLE**

Si parla di CHOSEN CIPHERTEXT ATTACK poiché l'avversario non conosce le due chiavi ... però conosce due blocchi $(P_1, C_1), (P_2, C_2)$.

L'avversario lavora "nel mezzo": prova tutte le possibili chiavi (2^{56} nel caso del DES) ... L'attacco ha successo quando c'è match!

CIFRATURA A 3-FASI

È una conseguenza della debolezza sopradescritta ... su cui si fonda il **3-DES**.



In realtà il 3-DES nasce per avere 3 chiavi

che porterebbe a 2^{3n} possibili chiavi ... e come abbiamo visto precedentemente, ciò non è necessario

Infatti, il 3-DES utilizza 3 chiavi, di cui però solo 2 sono diverse. Generalmente $K_1 = K_3$. K_2 è usato in modalità DECRYPTION.
Si parla infatti di DED-ENCRYPTION DECRYPTION ENCRYPTION

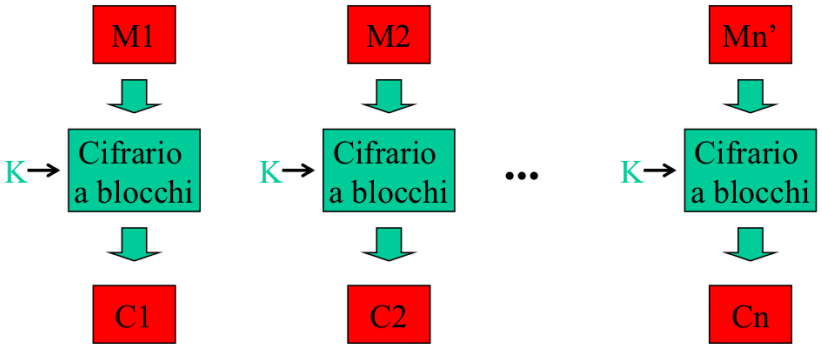
Questo ha anche una rilevanza a livello implementativo (si pensi in ambito software/hardware), poiché nel caso di $K_1 = K_2 = K_3$ ci si riporta al DES ... poiché è come se si cifrasse una volta sola:

CIFRO K_1 ⟶ CIPHERTEXT C_1
DECIFRO $K_2 = K1$ ⟶ PLAINTEXT P_1
CIFRO $K_3 = K_1$ ⟶ CIPHERTEXT C_1

TESTI PIU' LUNGHI

Concentriamoci sul 2° problema: Posso cifrare una informazione di lunghezza variabile?

L'idea è dividere il testo in BLOCCHI e CIFRARE ogni blocco:
ELECTRONIC CODEBOOK (ECB)



PROBLEMA 1: BLOCCO DI DIMENSIONE INFERIORE

Suddividendo il testo in blocchi, può capitare che un blocco sia inferiore rispetto alla dimensione richiesta dal cifrario

SOLUZIONE

SOLUZIONE 1: BIT RIEMPITIVI (PADDING DI 0)

NEW PROBLEM

PROBLEMA 1.1: n-BIT

come faccio a sapere quanti bit ho aggiunto? ...

PROBLEMA 2: ATTACCO DI FORZA BRUTA

Le regolarità nel testo in chiaro si ripetono nel testo cifrato e sarà quindi possibile una ANALISI STATISTICA

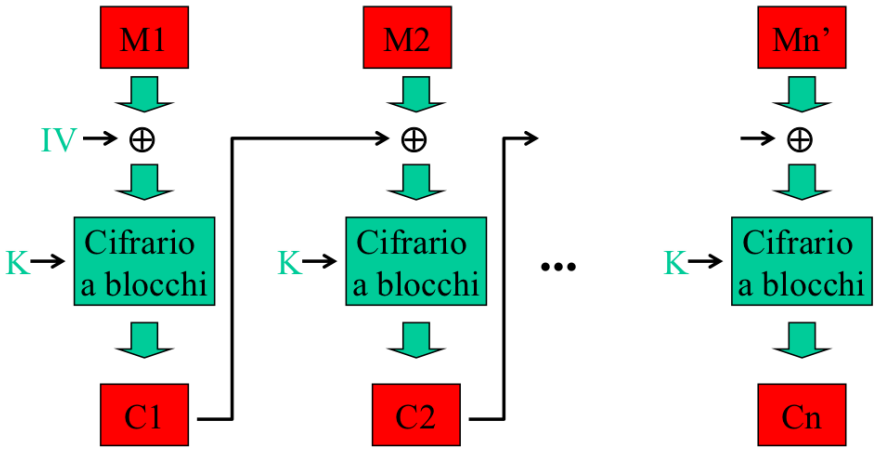
SOLUZIONE

SOLUZIONE 2: CIPHER BLOCK CHAINING (CBC)

Concatena i blocchi cifrati! Ampiamente usato con il DES, si parla di **3-DES-DED-CBC**

IV Initialization Vector

usato per il 1° passo, grande quanto un blocco



NEW PROBLEMS

PROBLEMA 2.1: ERRORE DI TRASMISSIONE

Un errore di trasmissione di un solo bit rende impossibile decifrare il corrispondente blocco e il blocco immediatamente successivo.

PROBLEMA 2.2: EFFICIENZA

Ad esempio per avere M2 devo prima avere C1 ...

NEW SOLUTION?

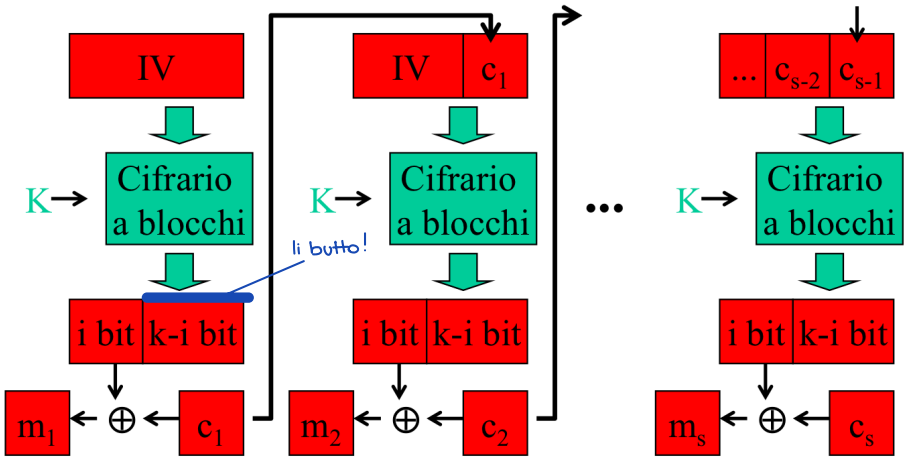
SOLUZIONE 3: CIPHER FEEDBACK (CFB)

risolve il precedente PROBLEMA 2.2

Trasforma il CIFRARIO A BLOCCHI in un CIFRARIO A FLUSSO, rendendo possibile la cifratura in tempo reale e il superamento del limite imposto dalla lunghezza del blocco.

Cifro l'Initialization Vector che divido in due parti (settabili).

Gli i bit significativi (il numero di bit è settabile) vengono dati in pasto ad uno XOR insieme al testo in chiaro c_1



SOLUZIONE 4: MODALITÀ OUTPUT FEEDBACK (OFB)

È meno efficiente del CBC però risolve il precedente PROBLEMA 2.1:

Un errore di trasmissione di un bit, rende indecifrabile il solo gruppo di i bit locale

Il resto del testo può essere decifrato

unica differenza rispetto al CFB