CRITTOGRAFIA: raccolta di esercizi d'esame (DES, AES).

Esercizio 1

1. Sia C una sequenza ottenuta rappresentando in binario ciascuna delle due cifre centrali del numero di matricola del candidato, prendendo per ciascuna di esse i tre bit meno significativi e concatenando questi due gruppi di tre bit. Nella fase i-esima del DES, C costituisca la parte iniziale della sequenza in ingresso della S-box. **Indicare** la sequenza C.
2. **Indicare** (con interi crescenti tra 1 e 32) la sequenza POS di posizioni dei bit di D[i] influenzati da C **spiegando** come è stato ottenuto il risultato.
3. Posto che la parte sinistra S[i-1] del messaggio entrante nella fase i sia una sequenza di 1, **indicare** il valore dei bit di D[i] di cui alla domanda precedente, **riportando** i calcoli eseguiti.

Esercizio 2

Si trasformi il sistema DES complementando tutte le uscite della S-box.
Sia M il proprio numero di matricola. Si converta M in una sequenza binaria B trasformando ordinatamente in binario ogni cifra decimale di M e prendendo per ciascuna di esse i tre bit meno significativi. Si estenda B fino a contenere in totale 48 bit aggiungendovi zeri a destra: tale sequenza sia l'uscita del blocco EP del DES, con chiave *k[0] =1010…10*.

1. **Indicare** la sequenza B.
2. Nella fase 1 del DES **determinare** il valore dei primi 4 bit a sinistra in uscita dalla S-box, **spiegando come è stato ottenuto il risultato.**
3. **Commentare** se il DES così modificato appaia o meno palesemente meno sicuro della versione standard.

Esercizio 3

Nella fase i-esima del DES siano 000011 i primi 6 bit a sinistra in ingresso alla S-box.

1. **Indicare** (con interi crescenti tra 1 e 32) la sequenza POS di posizioni dei bit di S[i+1]influenzati da questi 6 bit, **spiegando come è stato ottenuto il risultato**.
2. Siano c_1 c_2 …. i bit di S[i-1] nelle posizioni indicate in POS (le stesse quindi di S[i+1]). c_1 c_2 …. rappresentino in binario il numero di consonanti presenti nel nome e cognome del candidato. **Indicare** il valore dei bit di S[i+1] nelle posizioni POS **spiegando come è stato ottenuto il risultato**.

Esercizio 4

La S-box del cifrario AES è composta da 16 blocchi a 8 ingressi e 8 uscite ciascuno. Qual è il numero totale di possibili funzioni che si potrebbero scegliere per costruire ciascun blocco?

Esercizio 5

Detto X un arbitrario numero in decimale, si indichi con Xb la sequenza binaria ottenuta sostituendo ogni cifra di X con la sua trasfornmazione in binario su 4 bit.
Sia: D = 27062006 la data odierna, M = proprio numero di matricola seguito da 17.

1. Si calcolino Db e Mb.
2. In ogni fase del DES si mettono in XOR due sequenze di 32 bit: la parte a sinistra S del messaggio, e l'uscita U di una permutazione P di ingresso I (la tabella della P è indicata sotto). Ponendo S = Db e I = Mb, indicare l'uscita dello XOR mostrando i calcoli eseguiti.

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Esercizio 6

La proprietà di non linearità di qualsiasi cifratura a blocchi è fondamentale per la sua sicurezza. Infatti, si supponga di avere una cifratura lineare a blocchi *Cl* che cifra blocchi di 128 bit di testo in chiaro in 128 bit di testo cifrato, usando una chiave *k* (la lunghezza di k è irrilevante). Dunque, per ogni coppia di messaggi m_1 *e* m_2 risulta

$$Cl(m_1 \oplus m_2, k) = Cl(m_1, k) \oplus Cl(m_2, k).$$

Descrivere come un avversario che abbia 128 *testi cifrati scelti* possa decifrare qualsiasi testo cifrato senza conoscere la chiave segreta *k*.

NOTA: "testo cifrato scelto" significa che l'avversario ha la possibilità di scegliere un testo cifrato e ottenerne la decifrazione. In questo caso si hanno 128 coppie di testo in chiaro/testo cifrato e si ha la possibilità di scegliere i testi cifrati.

Esercizio 7

DESX è un cifrario proposto da Rivest per proteggere il DES dagli attacchi esaurienti. DESX usa una chiave segreta *w* di 64 bit oltre alla chiave DES *k* di 56 bit, e opera nel modo seguente:

$$C_{\text{DESX}}(m, k, w) = \text{w} \oplus C_{\text{DES}}(m \oplus w, k).$$

Mostrare come eseguire la decifrazione.

Esercizio 8

Si consideri un cifrario simmetrico a blocchi. Nel metodo FSM (Fischer Spiffy Mixer) ogni blocco *mi* del messaggio in chiaro viene cifrato come

$$c_i = m_{i-1} \oplus C(m_i \oplus c_{i-1}, k), \qquad i \geq 1$$

sando due sequenze di inizializzazione fissate (e pubbliche) m_0 e c_0.

1. Descrivere come eseguire la decifrazione di un blocco.
2. Nel caso in cui il blocco di crittogramma *ci* si danneggi nel corso della trasmissione , quali blocchi di testo in chiaro diventano indecifrabili?

Esercizio 9

Descrivere il cifrario AES, e in particolare le quattro operazioni eseguite in ciascuna fase.