CRITTOGRAFIA: raccolta di esercizi d'esame (funzioni hash, MAC, firma digitale).

Esercizio 1
Spiegare che proprietà devono possedere le funzione hash one-way, e perché tali funzioni sono importanti nei protocolli di autenticazione e di firma.

Esercizio 2
Si scriva un messaggio a piacere in italiano: $m = m_{20}\, m_{19}\, ...m_0$ costituito di 21 caratteri alfabetici più lo spazio.
Si consideri il sottoinsieme dell'alfabeto: $C_0 = \{A, B, \ldots, L\}$.
Utilizzando la chiave $k = k_5\, k_4\, k_3\, k_2\, k_1\, k_0$ consistente nelle 6 cifre decimali del proprio numero di matricola, si autentichi m mediante il MAC di 6 bit $A(m,k) = h_5\, h_4\, h_3\, h_2\, h_1\, h_0$ costruito come segue:

$j \leftarrow 0$
for i $\leftarrow$ 0 **to** 5 **do**
  $j \leftarrow [k_i + j]_{mod\ 21}$
  if $m_j \in C_0$ **then** $h_i \leftarrow 0$ **else** $h_i \leftarrow 1$.

1. **Riportare** i valori di m e h_i per $i = 0, 1,\ldots 5$, **indicando i calcoli eseguiti**.
2. **Spiegare** se la funzione A definita sopra è adatta per l'applicazione considerata.

Esercizio 3
Sia S la somma delle sei cifre decimali del numero di matricola qui sopra. Si ponga M = S+10.
Si convertano le cifre di M in binario su 4 bit, se ne calcoli lo EXOR e si riconverta il valore ottenuto in un numero decimale H che sarà usato come hash di M: h(M)=H.
Per due utenti Alice e Bob di un sistema RSA si considerino i seguenti insiemi di parametri.
Alice: p = 5, q = 11, e = 7, d = 23.
Bob: p = 7, q = 13, e = 5, d = 29.
Alice deve spedire a Bob il messaggio M cifrato e firmato in hash, impiegando le chiavi RSA e la funzione hash di cui sopra.
1. Spiegare se i parametri RSA indicati sopra sono scelti in modo consistente con le regole del cifrario (a parte le loro dimensioni).
2. Indicare esplicitamente tutte le operazioni aritmetiche eseguite da Alice e Bob nella trasmissione e verifica del messaggio M e della firma.

Esercizio 4
Posto che si scopra un algoritmo polinomiale per calcolare la funzione di Eulero, **spiegare** in termini matematici quale influenza la scoperta avrebbe sui protocolli di firma.

Esercizio 5
Sia $n = pq$, con p e q numeri primi, e sia e un intero coprimo con $\phi(n)$. Si discuta se la funzione

$$h(m_1, m_2) = m_1^e\, m_2^e \mod n$$

è resistente alle collisioni.

Esercizio 6

Due utenti A, B di un sistema RSA hanno scelto le seguenti chiavi: k[pub-A] = < 7, 341>; k[priv-A] = <43>; k[pub-B] = < 5, 299>; k[priv-B] = <53>. L'utente A deve spedire a B il seguente messaggio M cifrato e firmato in hash, impiegando le chiavi RSA e la seguente funzione hash *h*:

M = numero di matricola del candidato diviso in tre blocchi M1, M2, M3 di due cifre ciascuno.

h(M) = (M1+M2+M3) mod 100.

1. Spiegare se le chiavi di A e B sono scelte in modo consistente con le regole del cifrario (a parte le loro dimensioni), indicando i calcoli eseguiti.

2. Indicare esplicitamente tutte le operazioni aritmetiche eseguite da A e B nella trasmissione e verifica del messaggio M e della firma.

Esercizio 7

1. Siano M_1, M_2 gli interi costituiti rispettivamente dalle prime tre cifre e dalle ultime tre cifre del numero di matricola M qui sopra.
2. Sia B il massimo numero primo tale che: **if** $M_2 < 500$ **then** $B < M_2/30+20$ **else** $B < M_2/60 + 20$.
3. Si stabilisca un cifrario RSA con valore di *e* a scelta del candidato, *p* = B, *q* = 7.
4. Si convertano in binario i numeri M_1, M_2 e si consideri lo hash ottenuto come EXOR bit a bit tra sequenze: $h(M) = M_1 \oplus M_2$.
5. Si costruisca la firma in hash di M e si indichi come verificarla, usando il cifrario e la funzione h suddetti.

Riportare esplicitamente tutte le operazioni aritmetiche eseguite.

Esercizio 8

Si presenta un primo tentativo di firma elettronica basato su curve ellittiche. Si ha una curva ellittica globale, un numero primo *p*, e un "*generatore*" B. Alice sceglie una chiave di firma privata x_A e crea la chiave pubblica di verifica $Y_A = x_A B$. Per firmare un messaggio *M*:

- Alice sceglie un valore *k*
- Alice invia a Bob *M, k* e la firma $F = M - k\, x_A\, B$
- Bob verifica che $M = F + k\, Y_A$

1. Dimostrare che questo schema funziona correttamente. Ovvero che il processo di verifica produce un'uguaglianza quando la firma è valida.
2. Dimostrare che lo schema è inaccettabile descrivendo una semplice tecnica per creare la firma falsa di un utente su un qualsiasi messaggio.

Esercizio 9

Si presenta un tentativo di firma elettronica basato su curve ellittiche. Si ha una curva ellittica globale, un numero primo *p*, e un "*generatore*" B. Alice sceglie una chiave di firma privata x_A e crea la chiave pubblica di verifica $Y_A = x_A B$. Per firmare un messaggio *M*:

- Bob sceglie un valore *k*
- Bob invia ad Alice $C = k\, B$
- Alice invia a Bob *M* e la firma $F = M - x_A\, C$
- Bob verifica che $M = F + k\, Y_A$

1. Dimostrare che questo schema funziona correttamente. Ovvero che il processo di verifica produce un'uguaglianza quando la firma è valida.
2. Dimostrare che falsificare una firma con questo schema è difficile quanto forzare la crittografia a curva ellittica ElGamal.