

## 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.

Vedi testo, e uso delle funzioni hash nei protocolli di autenticazione e firma

### Esercizio 2

Si scriva un messaggio a piacere in italiano:  $m = m_{20} m_{19} \dots m_0$  costituito di 21 caratteri alfabetici più lo spazio.

Si consideri il sottoinsieme dell'alfabeto:  $C_0 = \{A, B, \dots, L\}$ .

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 ← 0  
for i ← 0 to 5 do  
    j ← [ki + j]mod 21  
    if mj ∈ C0 then hi ← 0 else hi ← 1.
```

1. Riportare i valori di  $m$  e  $h_i$  per  $i = 0, 1, \dots, 5$ , 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 riconverte 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.

L'algoritmo permetterebbe di calcolare in tempo polinomiale le chiavi private di un utente e dunque di falsificare le firme

### 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

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

è resistente alle collisioni.

NON è resistente. Infatti prendendo, ad esempio, le coppie  $(m_1, m_2) = (m_2, m_1)$  si ottiene una collisione con la coppia  $(m_1, m_2)$ .

### Esercizio 6

Due utenti A, B di un sistema RSA hanno scelto le seguenti chiavi:  $k[\text{pub-A}] = <7, 341>$ ;  $k[\text{priv-A}] = <43>$ ;  $k[\text{pub-B}] = <5, 299>$ ;  $k[\text{priv-B}] = <53>$ . 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.

$h(M) = (M_1 + M_2 + M_3) \bmod 100$ .

**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.

## ESEMPIO 2

$m = \text{SI SCRIVA UN MESSAGGI}$   
 $m_1 m_2 m_3 m_4 \dots \dots \dots m_3 m_2 m_1 m_0$

MATRICE:  $\begin{matrix} 6 & 5 & 4 & 3 & 2 & 1 \\ k_5 & k_4 & k_3 & k_2 & k_1 & k_0 \end{matrix}$

(1)

MAC:  $h_5 h_4 h_3 h_2 h_1 h_0$

$i=0$

$$j = (0 + k_0) \bmod 21 = 1$$

$$m_1 = G \in G_0 \Rightarrow h_0 = 0$$

$i=1$

$$j = (1 + k_1) \bmod 21 = (1+2) \bmod 21 = 3$$

$$m_3 = A \in G_0 \Rightarrow h_1 = 0$$

$i=2$

$$j = (3 + k_2) \bmod 21 = 6$$

$$m_6 = E \in G_0 \Rightarrow h_2 = 0$$

$i=3$

$$j = (6 + k_3) \bmod 21 = 10$$

$$m_{10} = U \notin G_0 \Rightarrow h_3 = 1$$

$i=4$

$$j = (10 + k_4) \bmod 21 = 15$$

$$m_{15} = R \notin G_0 \Rightarrow h_4 = 1$$

$i=5$

$$j = (15 + k_5) \bmod 21 = 0$$

$$m_0 = I \in G_0 \Rightarrow h_5 = 0$$

}

$$\text{MAC} = h_5 h_4 h_3 h_2 h_1 h_0$$

$$= 0 \mid 1 \mid 0 \mid 0 \mid 0$$

(2)

No, in quanto è possibile sostituire o alterare il messaggio senza cambiare il MAC, anche fermo consente la chiave  $k$ .

Inoltre è sufficiente sostituire le lettere del messaggio  $c_k \in G_0$  con una qualsiasi lettera di  $G_0$  e le lettere  $\notin G_0$  con lettere  $\notin G_0$ .

## ESERCIZIO 3

Matricola = 654321

$$S = 6+5+4+3+2+1 = 21$$

$$M = S+10 = 31$$

$$\begin{array}{r} 3 \rightarrow 011 \\ 1 \rightarrow 001 \end{array}$$

$$011 \oplus 001 = 010$$

$$\Rightarrow H = h(M) = h(31) = (010)_2 = 2$$

### 1. Alice

$$p=5, q=11, e=7, d=23$$

$$n=55, \phi(n)=40$$

$$\text{MCD}(e, \phi(n)) = \text{MCD}(7, 40) = 1$$

$$e \cdot d \bmod \phi(n) = 7 \cdot 23 \bmod 40 = 1 \quad \checkmark$$

### Bob

$$p=7, q=13, e=5, d=29$$

$$n=91, \phi(n)=72$$

$$\text{MCD}(e, \phi(n)) = \text{MCD}(5, 72) = 1$$

$$e \cdot d \bmod \phi(n) = 5 \cdot 29 \bmod 72 = 1 \quad \checkmark$$

### 2. Trasmissione e verifica di M e della firma (Protocollo 3: m cifrato e firmato in hash)

#### Alice

$$M = 31 \quad H = h(M) = 2$$

$$f = \mathbb{G}(H, k_{\text{Alice}}(\text{priv})) = 2^{23} \bmod 55 = 8$$

$$c = \mathbb{G}(M, k_{\text{Bob}}(\text{pub})) = 31^5 \bmod 91 = 5$$

→ Alice spedisce  $\langle \text{Alice}, 5, 8 \rangle$  a Bob

Bob

Riceve C e f da Alice.

Decifra C:

$$M = D(C, k_{\text{Bob}}[\text{priv.}]) = 5^{29} \pmod{91} = 31$$

Calcola  $h(M) = 2$

Verifica la firma di Alice:

$$G(f, k_{\text{Alice}}[\text{pubb.}]) = 8^7 \pmod{55} = 2$$

Con riuscita di ottenere  $h(M)$ . ✓

## ESEMPIO 6

1. A

$$n = 341 = 11 \times 31$$

$$\phi(n) = 10 \times 30 = 300$$

$$e = 7, \quad \text{MCD}(7, 300) = 1;$$

$$d = 43, \quad e \times d \pmod{\phi(n)} = 7 \times 43 \pmod{300} = 1 \quad \checkmark$$

B

$$n = 299 = 13 \times 23$$

$$\phi(n) = 12 \times 22 = 264$$

$$e = 5, \quad \text{MCD}(5, 264) = 1;$$

$$d = 53, \quad e \times d \pmod{\phi(n)} = 5 \times 53 \pmod{264} = 1 \quad \checkmark$$

## 2. Firma e cifratura

A: 1) calcola  $h(M) = 29$

2) genera  $f = 29^{43} \pmod{341}$

3) calcola  $C = C_1 C_2 C_3$

con  $C_1 = 65^5 \pmod{299}$

$$C_2 = 43^5 \pmod{299}$$

$$C_3 = 21^5 \pmod{299}$$

(dimensione dei blocchi =  $\lceil \log_2 299 \rceil = 8 \text{ bit}$ )

## Decifratura e verifica della firma

B: 1) decifra  $C_1 C_2 C_3$ , e trova  $M$

2) calcola  $h(M) = 29$

3) verifica la firma

$$G(f, k[\text{pub-A}]) \in$$

controllando di ottenere 29.

## ESERCIZIO 7

$$M = 654321$$

1)  $M_1 = 654$        $M_2 = 321$

2)  $M_2 < 500 \Rightarrow$  scegliere essere il massimo numero primo  $B$  t.c.

$$B < \frac{M_2}{30} + 20 = \frac{321}{30} + 20 = 30$$

$$\Rightarrow B = 29$$

3)  $p = 29$ ,  $q = 7$

$$n = 203, \quad \phi(n) = 168, \quad e = 5, \quad \text{NCD}(5, 168) = 1$$

$$d = 5^{-1} \bmod 168 = 101$$

4)  $M_1 = (654)_{10} = (1010001110)_2$   
 $M_2 = (321)_{10} = (0101000001)_2$

---

$$h(M) = (1111001111)_2$$

- 5) Si firma  $h(M)$  con la chiave privata di A (dividendo  $h(M)$  in bloccini se necessario)  
La verifica si esegue con la chiave pubblica di A, dopo aver ricalcolato  $h(M)$ .

### ESERCIZIO 8

1)  $F + k\gamma_A = (M - kx_A B) + k\gamma_A =$   
 $= M - kx_A B + k\gamma_A B = M$  ✓

2) Lo schema non è accettabile.

In fatti

$$F = M - k \cdot x_A \cdot B = M - k \cdot \gamma_A$$

-  $k$  è scelto da chi firma e  $\gamma_A$  è la chiave pubblica ~~di~~ di chi firma

### ESERCIZIO 9

1)  $F + k\gamma_A = (M - x_A C) + k\gamma_A = M - x_A k/B + k \cdot x_A \cdot B$

2)

Per falsificare la firma occorre calcolare

$$x_A \cdot C = x_A \cdot k \cdot B = k Y_A$$

$Y_A$  è pubblico, ma  $k$  non è noto.

Per ~~essere~~ ricavarlo da  $C = k B$  occorre

risolvere il problema del logaritmo discreto  
su curve ellittiche.

L'alternativa consiste nel calcolare la chiave  
privata  $x_A$  da  $Y_A$ , per cui occorre di nuovo  
risolvere il problema del logaritmo discreto su  
curve ellittiche.