

# Sicurezza delle Reti

Prof. Stefano Bregni

III Appello d'Esame 2021-22 – 9 settembre 2022

Cognome e nome:

(stampatello)  
(firma leggibile)

Matricola:

NB: In ogni esercizio, ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo.

## Domanda 1

(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il sistema di firma elettronica di El Gamal e pubblica  $p = 109$ ,  $\alpha = 9$ ,  $\beta = \alpha^a \bmod p$ , tenendo segreto l'esponente  $a = 64$ .

- Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se  $\alpha = 9$  non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme  $\alpha = \{2, 10\}$ . Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare  $\beta$ .
- Bob estrae il numero casuale segreto (*nonce*)  $k = 5$ . Per questo valore di  $k$ , calcolare la firma di Bob  $A = (r, s)$  del messaggio  $P = 100$ .
- Verificare se anche la firma  $A' = (r', s') = (6, 28)$  è valida da Bob per lo stesso messaggio  $P = 100$ .
- Se è valida, calcolare il valore di  $k$  per cui è stata calcolata da Bob, scegliendo il metodo più veloce a disposizione.

a)  $p$  primo  $1 < \alpha < p-2$   $k \perp p-1$   $p-1 = 108 = 2^2 \cdot 3^3$   
 $\left. \begin{array}{l} 10^{54} \equiv -1 \\ 10^{36} \equiv 63 \end{array} \right\} \Rightarrow \alpha = 10 \text{ (OK)} \quad (\alpha = 2, 9 \text{ NO})$   
Test se  $\alpha$  elem. prim. di  $\mathbb{Z}_p^*$ :  
 $\alpha^{(p-1)/q_i} \not\equiv 1 \pmod{p}$

b)  $r = \alpha^k \bmod p = 10^5 \bmod 109 = 47$   
 $s = k^{-1}(P - ar) \bmod (p-1) = 65 (100 - 64 \cdot 47) \bmod 108 = 88$   
 $k^{-1} \equiv 5^{-1} \equiv 65 \pmod{108}$   
 $\Rightarrow A = (47, 88)$   
 $\beta = \alpha^a \bmod p = 10^{64} \bmod 109 = 80$

c)  $\beta^r \cdot r^s \equiv \alpha^P \pmod{p}$   
 $80^6 \cdot 6^{28} \equiv 26 \pmod{109} \Rightarrow A' = (6, 28) \text{ firma valida di } P = 100$   
 $10^{100} \equiv 26 \quad (\sim)$

d) Invece di risolvere  $10^K \equiv 6 \pmod{109}$ , meglio:

$$5K \equiv P - \alpha r \pmod{(p-1)}$$

$$28K \equiv 100 - 64 \cdot 6 \pmod{108}$$

$$28K \equiv 40 \pmod{108}$$

$$\gcd(28, 108) = 4$$

$$8K \equiv 10 \pmod{27} \quad 7^{-1} \equiv 4 \pmod{27} \Rightarrow 4 \text{ soluzioni}$$

$$K_0 \equiv 10 \cdot 4 \equiv 13 \pmod{27}$$

$$K_i \equiv 13, 40, 67, 94 \pmod{108}$$

$$\Rightarrow K = 13$$

Dei dati pubblici:

$$\alpha^K \equiv r \pmod{p}$$

$$10^K \equiv 6 \pmod{109}$$

## Domanda 2

(svolgere su questo foglio nello spazio assegnato) (7 punti)

Bob adotta il sistema di cifratura a chiave pubblica di El Gamal e pubblica  $p = 199$ ,  $\alpha = 3$ ,  $\beta = \alpha^a \bmod p$ , tenendo segreto l'esponente  $a = 32$ .

- Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se  $\alpha = 3$  non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme  $\alpha = \{3, 4\}$ . Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare  $\beta$ .
- Alice estrae il numero casuale segreto (*nonce*)  $k = 29$  e spedisce il messaggio  $P = 50$  a Bob. Calcolare il messaggio cifrato  $C = (r, t)$ .
- Bob riceve  $C' = (r', t') = (34, 8)$ . Calcolare il messaggio decifrato da Bob  $P'$ .
- Calcolare il valore di  $k$  per cui Alice ha calcolato  $C' = E[P]$ .

a)  $p$  primo  $1 < \alpha < p-1$   $p-1 = 198 = 2 \cdot 3^2 \cdot 11$  Teste di elem. pr. di  $\alpha^{p-1} \equiv 1 \pmod{p}$   $\mathbb{Z}_p^*$

$$\left. \begin{array}{l} 3^{99} \equiv -1 \\ 3^{66} \equiv 106 \\ 3^{18} \equiv 125 \end{array} \right\} \begin{array}{l} \alpha = 3 \quad (\alpha = 4 \text{ No}) \\ \text{OK} \end{array} \quad \beta = \alpha^a \bmod p = 3^{32} \bmod 199 = 102$$

b)  $r = \alpha^k \bmod p = 3^{29} \bmod 199 = 49$   
 $t = \beta^k P \bmod p = 102^{29} \cdot 50 \bmod 199 = 72 \Rightarrow C = (49, 72)$

c)  $P' = t' \cdot r'^{-1} \bmod p = 8 \cdot 34^{-32} \bmod 199 = 23$

d)  $3^k \bmod 199 = 34 \rightarrow (k=31) \text{ (BSGS)}$

**Domanda 3**

(svolgere su questo foglio nello spazio assegnato) (7 punti)

- a) Avete scelto una funzione di *hash* che restituisce valori di lunghezza  $L = 16$  bit. In una tabella, avete memorizzato i valori di *hash* calcolati su un milione di file diversi. Qual è la probabilità che almeno due di questi file abbiano lo stesso hash in tabella?

$$N = 2^{16} = 65536$$
$$r = 10^6$$
$$P \approx 1 - e^{-r^2/2N} = 1$$

- b) Spiegare cosa significa affermare che una generica funzione  $y = y(x)$  è invertibile, ma unidirezionale. Spiegare cosa significa affermare che una funzione di hash  $y = y(x)$  (non invertibile!) è non unidirezionale.

Funzione invertibile ma unidirezionale:

Questa affermazione è contraddittoria e non può essere vera.

- Una funzione è invertibile se, dato  $y$ , è possibile trovare facilmente un unico  $x$  tale che  $y = y(x)$ .- Una funzione è unidirezionale se è facile calcolare  $y$  da  $x$ , ma difficile o praticamente impossibile invertire e risalire a  $x$  da  $y$ .

Quindi:

Se una funzione è invertibile, non è unidirezionale. Se è unidirezionale, non è invertibile.

Funzione di hash non invertibile e non unidirezionale:

Una funzione di hash è non invertibile perché comprime input di lunghezza arbitraria in output a lunghezza fissa; quindi non c'è una corrispondenza uno a uno.

Dire che è non unidirezionale significa che è possibile trovare un input  $x$  a partire da un valore  $y = y(x)$ .

In pratica, la funzione può essere invertita con un certo sforzo computazionale o facilmente, quindi non protegge il dato originale.

Questo compromette la sicurezza, perché chi conosce l'hash può risalire al messaggio originario.

- c) Sappiamo che una certa funzione di hash  $h = h(x)$  non è unidirezionale.

Dato un valore di hash  $h$ , potrebbe quindi essere possibile ricavare il messaggio  $m$  da cui è stato calcolato? Perché?Sì, se una funzione di hash  $h = h(x)$  non è unidirezionale, allora dato un valore di hash  $h$  è possibile trovare almeno un messaggio  $m$  tale che  $h = h(m)$ .

Questo accade perché:

Una funzione unidirezionale rende difficile o praticamente impossibile risalire a un input partendo dall'hash.

Se invece la funzione non è unidirezionale, esiste un metodo efficiente per trovare un messaggio  $m$  che produce quel valore di hash.

Quindi, la mancanza di unidirezionalità implica che l'inversione della funzione è facile o possibile.

- d) Si consideri una ipotetica funzione di hash  $h = h(m) = m^7 \bmod p$ , dove  $p$  è un primo tale per cui il problema del logaritmo discreto sia intrattabile in  $\mathbb{Z}_p^*$  e  $m$  è un intero qualsiasi. Si spieghi perché tale funzione di hash  $h = h(m)$  è unidirezionale, ma non debolmente resistente alle collisioni.

Unidirezionalità:

- Calcolare  $h(m) = m^7 \bmod p$  è semplice.- Invertire la funzione, cioè trovare  $m$  dato  $h(m)$ , equivale a risolvere il logaritmo discreto di base 7 in  $\mathbb{Z}_p^*$ .- Poiché il problema del logaritmo discreto in  $\mathbb{Z}_p^*$  è considerato intrattabile, è computazionalmente difficile risalire a  $m$ , quindi la funzione è unidirezionale.

Non debole resistenza alle collisioni:

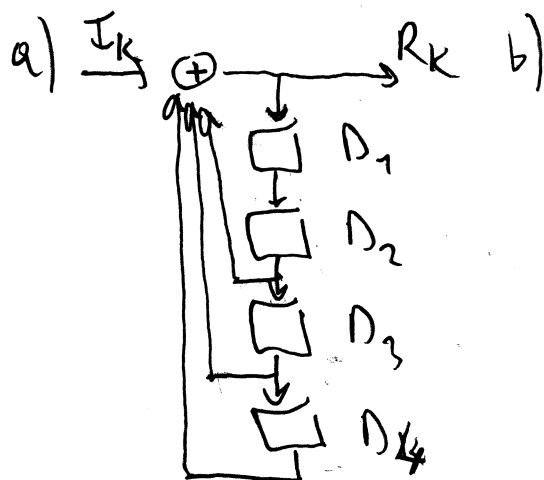
- La funzione è una potenza modulo  $p$ , quindi se l'ordine di 7 modulo  $p$  non è coprimo con  $p-1$ , cioè se esistono numeri  $k \neq 0$  tali che:  $m^7 = (m * g^{k * \text{ord}(a)})^7 \bmod p$  (dove  $g$  è un generatore),- Esistono valori distinti di  $m$  che producono lo stesso valore di  $h(m)$ .- In particolare, dato che 7 è un numero fisso e l'ordine del gruppo può dividere il ciclo, è facile trovare collisioni: ad esempio,  $m_1$  e  $m_2 = m_1 * r$ , con  $r^7 = 1 \bmod p$ , hanno lo stesso hash.

- Quindi è facile trovare collisioni, il che significa che la funzione non è resistente alle collisioni, nemmeno debolmente.

**Domanda 4**

(svolgere su questo foglio nello spazio assegnato) (4 punti)

- a) Si disegni lo schema di un generatore di sequenza PRBS basato su registro a scorrimento LFSR, realizzato come *scrambler autosincronizzante* con polinomio caratteristico  $P(x) = x^4 + x^3 + x^2 + 1$  alimentato con tutti "0". Si indichino la sequenza binaria in ingresso con  $\{I_k\} \equiv \{0\}$  e la sequenza binaria in uscita con  $\{R_k\}$ .
- b) Si inizializzino gli elementi di ritardo  $D_i$  ( $i = 1, 2, 3, 4$ ) con  $\{0, 1, 1, 1\}$  al passo iniziale  $k = 0$ . Ricavare la sequenza PRBS  $\{R_k\}$  generata all'uscita, evidenziando la sua periodicità. Qual è il periodo  $P$  della sequenza?
- c) Verificare se il polinomio  $P(x)$  è irriducibile. Perché è importante fare questa verifica?



b)

$k$	$I_k$	$D_{1k}$	$D_{2k}$	$D_{3k}$	$D_{4k}$	$R_k$
0	0	0	1	1	1	1
1	0	1	0	1	1	0
2	0	0	1	0	1	0
3	0	0	0	1	0	1
4	0	1	1	0	1	1
5	0	1	1	0	0	1
6	0	1	1	1	0	0
7	0	0	1	1	1	1

P=7

c)  $P(x) = x^4 + x^3 + x^2 + 1$

Divisibile per  $x$ ? no  
" per  $(x+1)$ ? si

$\Rightarrow P(x) = (x+1)(x^3 + x + 1)$

$$\begin{array}{r}
 \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + 1 \\
 \underline{\cancel{x^4} + \cancel{x^3}} \\
 \cancel{x^2} + 1 \\
 \underline{\cancel{x^2} + \cancel{x}} \\
 x + 1 \\
 \underline{x + 1} \\
 0
 \end{array}
 \quad
 \begin{array}{r}
 x + 1 \\
 \hline
 x^3 + \cancel{x} + 1
 \end{array}$$

Cognome e nome:

(stampatello)

(firma leggibile)

Matricola:

## Domanda 5

(rispondere su questo foglio negli spazi assegnati) (11 punti)

(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).

- 1) Si consideri un generatore di password consistenti di 8 simboli casuali scelti nell'alfabeto coreano, che comprende 19 consonanti e 21 vocali. Qual è la quantità di informazione [bit] delle password, se i simboli sono scelti indipendentemente una dall'altro, e la probabilità che siano una consonante o una vocale vale rispettivamente 30% e 70%? (2 punti)

$$H(X) = -\left(0,3 \log_2 \frac{0,3}{19} + 0,7 \log_2 \frac{0,7}{21}\right) = 5,23 \text{ bit/simbolo}$$

$$H(8 \text{ simboli}) = 41,84 \text{ bit}$$

- 2) Si calcolino tutti i residui quadratici dell'insieme  $\mathbb{Z}_{11}^*$ , partendo dalle potenze del suo elemento primitivo  $\alpha = 6$ . Esaminando i risultati ottenuti, si dica quali sono le radici quadrate di 5 (mod 11), se esistono. (2 punti)

$$6^0 \equiv 1 \pmod{11}$$

$$6^2 \equiv 3 \pmod{11}$$

$$6^4 \equiv 9 \pmod{11}$$

$$6^6 \equiv 5 \pmod{11}$$

$$6^8 \equiv 4 \pmod{11}$$

$$\alpha_9 = \{1, 3, 4, 5, 9\}$$

$$\Rightarrow \sqrt{5} \pmod{11} \equiv \pm 6^3 \equiv \pm 7 \equiv 4, 7$$

- 3) Cos'è l'ordine di un elemento  $\alpha \in \mathbb{Z}_p^*$ ? Cos'è un elemento primitivo dell'insieme  $\mathbb{Z}_p^*$ ?

(2 punti)

L'ordine di  $a$  è il minimo intero positivo  $k$  tale che  $a$  elevato alla  $k$  è congruente a 1 modulo  $p$ , cioè:  $a^k \equiv 1 \pmod{p}$ . In altre parole, è il più piccolo esponente  $k$  per cui tornando a 1 nel gruppo moltiplicativo modulo  $p$ .

Un elemento primitivo (o generatore) è un elemento  $a$  di  $\mathbb{Z}_p^*$  che ha ordine esattamente  $p-1$ .

Questo significa che: le potenze successive di  $a$  (da  $a^1$  a  $a^{p-1}$ ) generano tutti gli elementi non nulli di  $\mathbb{Z}_p^*$  senza ripetizioni prima di arrivare a 1.

4) Ricevi un certificato che tra le altre include le seguenti informazioni:

*Issuer name: VERISIGN;*

*Period of validity: from 1/1/1900 to 31/12/2199;*

*Subject name: MOZILLA;*

*Public Key of the Subject: XX;*

*Signature: YY.*

Che procedura segui per verificare l'autenticità del certificato?

(2 punti)

1. Verifica della firma digitale:

- Uso la chiave pubblica di Verisign (emittente, CA) nota e considerata affidabile.

- Controllo che la firma digitale YY sia correttamente generata applicando la funzione di verifica sulla parte firmata del certificato (Issuer, Subject, Public Key, etc).

- Se la verifica della firma fallisce, il certificato è falso o manomesso.

2. Controllo del periodo di validità:

- Verifico che la data corrente rientri nel periodo di validità del certificato (tra 1/1/1900 e 31/12/2199).

- Se la data è fuori dal periodo, il certificato non è valido.

3. Controllo della revoca:

- Consulto la Certificate Revocation List (CRL) o uso il protocollo OCSP per assicurarmi che il certificato non sia stato revocato da Verisign.

4. Verifica dell'identità del Subject:

- Controllo che il nome del Subject corrisponda all'entità attesa (in questo caso "MOZILLA").

- Ricordo però che un certificato valido non garantisce da solo che la comunicazione sia con MOZILLA, perché la chiave privata potrebbe essere compromessa o il certificato contraffatto se la CA è compromessa.

5) Con un browser web mi collego in modo sicuro a un sito alla URL <https://www.esempio.edu>. Dove prendo le chiavi per cifrare la mia comunicazione con il server? L'Amministratore della mia rete è a conoscenza o no del fatto che ho visitato il sito? Se il sito mi chiede una password di accesso, questa sarà leggibile dall'Amministratore della mia rete?

(3 punti)

1. Da dove prendo le chiavi per cifrare la comunicazione?

- Le chiavi di cifratura vengono generate tramite il protocollo TLS (Transport Layer Security).

- Durante la connessione, il server invia al browser il proprio certificato digitale, contenente la sua chiave pubblica.

- Il browser verifica il certificato e usa la chiave pubblica del server per negoziare una chiave simmetrica segreta da usare per cifrare la comunicazione successiva.

Questa chiave simmetrica viene concordata tramite algoritmi come Diffie-Hellman o usando la crittografia a chiave pubblica.

2. L'amministratore di rete sa che hai visitato il sito?

L'amministratore può sapere che hai contattato l'indirizzo IP del server [www.esempio.edu](https://www.esempio.edu), e quindi che hai visitato quel sito (o almeno quel server). Tuttavia, non può vedere i contenuti della comunicazione perché sono cifrati.

3. Se il sito chiede una password, l'amministratore la può leggere?

No, la password è trasmessa all'interno della connessione cifrata TLS, quindi l'amministratore non può leggerla in chiaro.

Solo il browser e il server possono accedere ai dati scambiati.