# Sicurezza delle Reti

**Prof. Stefano Bregni** **II Appello d'Esame 2021-22 – 21 luglio 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) (6 punti)*

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 131$, $\alpha = 8$, $\beta = \alpha^a \bmod p = 83$, tenendo segreto l'esponente $a$ ($1 < a \leq p\text{-}2$).

Bob estrae il numero casuale segreto $k$ (*nonce*) con MCD($k$, $p$-1) = 1. Usando sempre questo stesso valore di $k$, Bob calcola le seguenti firme $A_1$ e $A_2$ per i rispettivi messaggi $P_1$ e $P_2$.

$A_1 = (r_1, s_1) = (10, 85)$ $P_1 = 25$
$A_2 = (r_2, s_2) = (10, 30)$ $P_2 = 30$

Oscar intercetta i due messaggi firmati. Sulla base di essi e delle informazioni pubbliche, calcolare $k$ e $a$ (*attacco del nonce ripetuto*).

$s \equiv k^{-1}(P - ar) \pmod{(p-1)} \rightarrow sk \equiv P - ar \pmod{(p-1)}$

$$\begin{cases} 85k \equiv 25 - a\cdot 10 \pmod{130} \\ 30k \equiv 30 - a\cdot 10 \pmod{130} \end{cases}$$

$55k \equiv -5 \pmod{130}$ $\quad MCD(55,130) = 5 \Rightarrow 5$ soluzioni

$11k \equiv -1 \pmod{26}$ $\quad 11^{-1} \equiv -7 \pmod{26}$

$k_0 \equiv 7 \pmod{26}$ $\quad k_i \equiv 7, 33, 59, 85, 111 \pmod{130}$

$k = 59 \Leftarrow$ Dai dati pubblici $r \equiv \alpha^k \pmod{p}$
$10 \equiv 8^k \pmod{131}$

$30 \cdot 59 \equiv 30 - a10 \pmod{130}$

$10a \equiv 80 \pmod{130}$ $\quad MCD(10,130) = 10 \Rightarrow 10$ soluzioni

$a_0 \equiv 8 \pmod{13}$

$a_i \equiv 8, 21, 34, 47, 60, 73, 86, 99, 112, 125 \pmod{130}$

$\Rightarrow a = 47$ $\quad$ Dai dati pubblici: $\beta \equiv \alpha^a \pmod{p}$

$83 \equiv 8^a \pmod{131}$

**Cognome e nome:** *(stampatello)*
*(firma leggibile)*

**Matricola:**

**Domanda 2**
*(svolgere su questo foglio nello spazio assegnato) (7 punti)*

Bob adotta il *sistema di firma elettronica di El Gamal* e pubblica $p = 109$, $\alpha = 4$, $\beta = \alpha^a \bmod p$, tenendo segreto l'esponente $a = 32$.

a) Verificare la correttezza dei dati forniti, in base alle ipotesi del metodo di El Gamal. Se $\alpha = 4$ non risultasse una scelta valida, Bob userà invece un valore valido scelto nell'insieme $\alpha = \{5, 6\}$. Se nessuna di queste scelte risultasse valida, Bob rinuncerà a proseguire (e l'esercizio termina qui). Calcolare $\beta$.

b) Bob estrae il numero casuale segreto (*nonce*) $k = 35$. Per questo valore di $k$, calcolare la firma di Bob $A = (r, s)$ del messaggio $P = 25$.

c) Verificare se anche la firma $A' = (r', s') = (11, 39)$ è valida da Bob per lo stesso messaggio $P = 25$.

d) 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 $\quad 1 < \alpha < p-2 \quad k \perp p-1 \quad p-1 = 108 = 2^2 \cdot 3^3$

Test se $\alpha$ elem. prim. di $Z_p^*$:

$\alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$

$$\left.\begin{array}{l} 6^{54} \equiv -1 \\ 6^{36} \equiv 63 \end{array}\right\} \Rightarrow \alpha = 6 \text{ OK} \quad (\alpha = 4, 5 \text{ no})$$

$\beta = \alpha^a \bmod p = 6^{32} \bmod 109 = 22$

b) $r = \alpha^k \bmod p = 6^{35} \bmod 109 = 65$

$s = k^{-1}(P - ar) \bmod (p-1) = 71(25 - 32 \cdot 65) \bmod 108 = 3$

$k^{-1} \equiv 35^{-1} \equiv 71 \pmod{108} \quad \Rightarrow \boxed{A = (65, 3)}$

c) $\beta^r \cdot r^s \equiv \alpha^P \pmod p$

$22^{11} \cdot 11^{39} \equiv 10 \pmod{109}$

$6^{25} \equiv 10 \quad (\text{—})$

$\Rightarrow A' = (11, 39)$ firma valida di $P = 25$

d) Invece di risolvere $6^K \equiv 11 \pmod{109}$, meglio:

$sK \equiv P - ar \pmod{(p-1)}$

$39K \equiv 25 - 32 \cdot 11 \pmod{108}$

$39K \equiv 105 \pmod{108}$ $\quad MCD(39, 108) = 3 \Rightarrow 3$ soluzioni

$13K \equiv 35 \pmod{36}$ $\quad 13^{-1} \equiv 25 \pmod{36}$

$K_0 \equiv 35 \cdot 25 \equiv 11 \pmod{36}$

$K_i = 11, 47, 83 \pmod{108}$

$\Rightarrow K = 83$

Dai dati pubblici:

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

$6^K \equiv 11 \pmod{109}$

**Cognome e nome:** *(stampatello)*
*(firma leggibile)*

**Matricola:**

**Domanda 3**
*(svolgere su questo foglio nello spazio assegnato) (7 punti)*

a) Con che probabilità 2 messaggi casuali, di lunghezza rispettivamente 1024 bit e 2048 bit, hanno lo stesso hash SHA-2 256?

$2^{-256} \cong 0$

Assumiamo che la funzione di hash usata sia SHA-2 (es. SHA-256), che produce un output di 256 bit.
In generale, se una funzione di hash ha output di n bit, allora:
Ci sono 2^n possibili valori di hash, la probabilità che due messaggi casuali producano lo stesso hash (collisione) è 1 su 2^n, cioè:
Probabilità = 1 / 2^256
Questa probabilità è estremamente bassa, praticamente zero.

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*.

GIA FATTO

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?

GIA FATTO

d) Si consideri una ipotetica funzione di *hash* $h = h(m) = \alpha^m \bmod p$, dove $p$ è un primo tale per cui il problema del logaritmo discreto sia intrattabile in $\mathbb{Z}_p^*$, $\alpha$ è un elemento generatore di $\mathbb{Z}_p^*$, 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:
La funzione h(m) = a^m mod p è unidirezionale perché:
- È facile calcolare h(m) dato m (esponenziazione modulare).
- Ma è computazionalmente difficile invertire la funzione, cioè trovare m dato h(m),
- Perché ciò equivale a risolvere il logaritmo discreto in Z*_p: trovare m tale che a^m ≡ h mod p.
- Poiché il problema del logaritmo discreto è considerato intrattabile in Z*_p (se p è sufficientemente grande), non è fattibile ricavare m da h(m).
→ Quindi, la funzione è unidirezionale.

Non debolmente resistente alle collisioni:
La funzione non è debolmente resistente alle collisioni perché:
- Conoscendo un valore $m_1$, è facile trovare un altro $m_2 \neq m_1$ tale che $h(m_1) = h(m_2)$,
- Infatti, poiché a è un generatore di Z*_p, ha ordine p−1, quindi:
$h(m_1) = a^{m_1} \bmod p$
$h(m_2) = a^{m_2} \bmod p$
- Se $m_2 \equiv m_1 \bmod (p-1)$, allora $a^{m_2} \equiv a^{m_1} \bmod p$ → collisione.
Quindi, date le proprietà cicliche del gruppo moltiplicativo Z*_p, è semplice trovare collisioni conoscendo $m_1$,
→ La funzione non è nemmeno debolmente resistente alle collisioni.

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

a) Ricavare la sequenza binaria pseudo-casuale $\{x_i\}$ generata dall'algoritmo *Blum-Blum-Shab* per $p = 47$, $q = 59$, $x = 60$ e determinarne il periodo $P$. Il seme iniziale $x$ rispetta le ipotesi del metodo?

| $i$ | $x_i$ | $b_i$ |
|---|---|---|
| 0 | 827 | 1 |
| 1 | 1771 | 1 |
| 2 | 178 | 0 |
| 3 | 1181 | 1 |
| 4 | 2715 | 1 |
| 5 | 591 | 1 |
| 6 | 2656 | 0 |
| 7 | 2597 | 1 |
| 8 | 473 | 1 |
| 9 | 1889 | 1 |
| 10 | 2243 | 1 |
| 11 | 827 | 1 |
| 12 | | |

$P = 11$

$n = p \cdot q = 47 \cdot 59 = 2773$

$x_0 \equiv x^2 \pmod{n}$

$x_i \equiv x_{i-1}^2 \pmod{n}$

$47 \equiv 3 \pmod{4}$

$59 \equiv 3 \pmod{4}$

$60 \perp p \cdot q$

b) In base alla teoria, quali sono i valori possibili che può assumere il periodo $P = \pi(x_0)$ del generatore precedente, per valori arbitrari del seme $x_0 = x^2 \in \mathbb{Z}_n$?

Si ricorda che $\pi(x_0)$ divide $\lambda(\lambda(n))$, dove $\lambda(n)$ è la Funzione di Charmichael, calcolabile come

$$\lambda(n) = \mathrm{mcm}\left(\left\{\lambda\left(p_i^{a_i}\right)\right\}\right) \qquad \lambda\left(p^k\right) = \begin{cases} \frac{1}{2}\varphi\left(p^k\right) & \text{se } p = 2, k \geq 3 \\ \varphi\left(p^k\right) & \text{altrimenti} \end{cases}$$

$\lambda(n) = \mathrm{mcm}(46, 58) = 2 \cdot 23 \cdot 29 = 1334$

$\lambda[\lambda(n)] = \lambda(1334) = \mathrm{mcm}(1, 22, 28) = 308 \quad (= 2^2 \cdot 7 \cdot 11)$

$\pi(x_0) \in \{1, 2, 4, 7, 11, 14, 22, 28, 44, 77, 154, 308\}$

**Cognome e nome:** *(stampatello)*
*(firma leggibile)*

**Matricola:**

**Domanda 5**

*(rispondere su questo foglio negli spazi assegnati) (12 punti)*
*(NB: ogni risposta non giustificata adeguatamente, anche con pochissime parole, avrà valore nullo).*

**1)** Suggerire come trovare le radici dell'equazione $4 \equiv 3^x \pmod{77}$, se esistono. *(2 punti)*

L'equazione 4 ≡ 3·x (mod 77) è una congruenza lineare. Per risolverla, dobbiamo trovare x tale che: 3·x ≡ 4 mod 77
Passaggi per trovare la soluzione:
1. Verifica che il coefficiente 3 sia invertibile modulo 77:
- Calcola MCD(3, 77).
- Poiché 3 e 77 sono coprimi (MCD = 1), 3 ha un inverso modulo 77.
2. Trova l'inverso moltiplicativo di 3 modulo 77:
- Vogliamo un intero y tale che 3·y ≡ 1 mod 77.
- Usando l'algoritmo esteso di Euclide, troviamo: l'inverso di 3 modulo 77 è 26, perché: 3·26 = 78 ≡ 1 mod 77
3. Moltiplica entrambi i membri della congruenza per l'inverso:
(3·x)·26 ≡ 4·26 mod 77
⇒ x ≡ 104 mod 77
⇒ x ≡ 27 mod 77

**2)** In generale, è più difficile risolvere un *Problema Computazionale di Diffie-Hellman* o un *Problema del Logaritmo Discreto*? Perché? *(2 punti)*

In generale, il Problema del Logaritmo Discreto (DLP) è considerato più difficile del Problema Computazionale di Diffie-Hellman (CDHP).
Se riesci a risolvere il logaritmo discreto, puoi risolvere anche il problema di Diffie-Hellman.
Infatti, dato g, g^a e g^b, se trovi a risolvendo il logaritmo discreto (g^a → a), puoi calcolare g^{ab}.
Ma non vale il contrario: anche se riesci a calcolare g^{ab} (soluzione del CDHP), non necessariamente puoi ricavare a o b (quindi non risolvi il logaritmo discreto).
Conclusione:
Il Problema del Logaritmo Discreto è almeno tanto difficile quanto il problema di Diffie-Hellman.
Ma si ritiene più difficile in generale, perché risolverlo implica anche la soluzione del CDHP.
Quindi:
→ DLP ≥ CDHP in difficoltà computazionale.

**3)** A cosa serve il *Protocollo di Needham-Schroeder*? Quali sono gli attori? Viene eseguito allo scopo di produrre o trasferire quale informazione? *(2 punti)*

1. Scopo del protocollo:
Il Protocollo di Needham-Schroeder serve a permettere l'autenticazione reciproca tra due entità (ad esempio A e B) e a stabilire una chiave di sessione segreta condivisa tra loro.
La comunicazione avviene con l'aiuto di un server di autenticazione fidato.

2. Attori coinvolti:
A: primo partecipante (es. client)
B: secondo partecipante (es. server)
KDC (Key Distribution Center): il server fidato che genera e distribuisce le chiavi

3. Informazione prodotta o trasferita:
Il protocollo viene eseguito per produrre e trasferire una chiave di sessione (K_AB) tra A e B, in modo sicuro.
Questa chiave sarà poi usata da A e B per comunicare cifrando i messaggi tra loro.

**4)** Cos'è l'*ordine* di un elemento $\alpha \in \mathbb{Z}_p^*$? Elencare i valori possibili dell'ordine di un elemento $\alpha \in \mathbb{Z}_{149}^*$. *(2 punti)*

$\{1, 2, 4, 37, 74, 148\}$

L'ordine di un elemento a ∊ Z∗_p è il più piccolo intero positivo k tale che: a^k ≡ 1 mod p
In altre parole, è il numero di moltiplicazioni successive necessarie per far tornare a 1 modulo p.
L'ordine di a divide sempre p−1 (per il teorema di Lagrange).

149 è primo, quindi Z∗_149 è il gruppo moltiplicativo modulo 149.
L'ordine del gruppo è 149−1 = 148, quindi:gli ordini possibili degli elementi di Z∗_149 sono tutti i divisori di 148.

**5)** Sia data una funzione di hash $h = h(m)$ unidirezionale che restituisce valori pseudocasuali di lunghezza fissa 20 bit. Un attaccante tenta di ottenere un valore di hash desiderato $H$, calcolando la $h(m)$ su variazioni casuali di un messaggio malevolo $m$. Quanti tentativi sono necessari perché l'attacco abbia successo (si ottenga $h(m) = H$) con probabilità almeno 0.5? *(2 punti)*

$P = \left(1 - \frac{1}{2^{20}}\right)^n \cong (1 - n2^{-20})$

$P = \frac{1}{2} \rightarrow$ (approssimato) $1 - n2^{-20} = \frac{1}{2} \rightarrow n \cong 2^{19} = 524288$

(esatto) $(1 - 2^{-20})^n = \frac{1}{2}$ $\quad n \log(1 - 2^{-20}) = \log 1/2$

$\rightarrow n = 726817$

**6)** Trovare i fattori primi di $n = 22499$ attraverso l'*Algoritmo di Fattorizzazione p−1* di Pollard con base $a = 2$. *(2 punti)*

$b_1 \equiv 2 \pmod{22499}$

$b_2 \equiv 2^2 \equiv 4$ (——) $\qquad MCD(3, n) = 1$

$b_3 \equiv 4^3 \equiv 64$ (~) $\qquad MCD(63, n) = 1$

$b_4 \equiv 64^4 \equiv 15461$ (~) $\qquad MCD(15460, n) = 1$

$b_5 \equiv 15461^5 \equiv 2115$ (~) $\qquad MCD(2114, n) = 151$

$\Rightarrow p = 151$

$q = 149$