Computer Security

Esercizi

Indice

Crittografia basata sull'IFP 2
  RSA 2
    Chiavi 2
    Costruzione delle chiavi 2
    Cifratura e decrifratura 2
    Esempio 2
    Strategia *square-and-multiply* per le potenze 3
    Velocizzazione dello *square-and-multiply* usando il teorema cinese del resto 4
Crittografia basata sul DLP 5
  Diffie-Hellman 5
    Esempio 6
  ElGamal 7
    Chiavi 7
    Creazione delle chiavi 7
    Cifratura e decifratura 7
    Esempio di cifratura e decifratura 7
    Firme 9
    Esempio per la firma 9

Crittografia basata sull'IFP

RSA

Chiavi

Chiave pubblica :

$$k_{\text{pub}} = \langle e, n \rangle$$

Chiave privata:

$$k_{\text{priv}} = \langle p, q, \varphi(n), d \rangle$$

Costruzione delle chiavi

1. scegliere due primi p, q
2. calcolare $n = pq$
3. calcolare la funzione totiente di Eulero $\varphi(n) = (p-1)(q-1)$
4. scegliere e tale che $1 < e < \varphi(n)$, $\gcd(e, \varphi(n)) = 1$
5. calcolare d tale che $(de) \bmod \varphi(n) = 1$ usando la divisione euclidea oppure la formula basata sugli inversi $d = e^{-1} \bmod \varphi(n)$

Cifratura e decrifratura

Cifratura:

$$c = m^e \bmod n$$

Decifratura:

$$m = c^d \bmod n$$

Esempio

Creazione delle chiavi:

1. $p = 17$, $q = 23$
2. $n = pq = 17 \cdot 23 = 391$
3. $\varphi(n) = (p-1)(q-1) = 16 \cdot 22 = 352$
4. scegliamo $e = 43$, dato che $1 < 43 < 352$ e $\gcd(43, 352) = 1$
5. calcoliamo d tale che $(d \cdot 43) \bmod 352 = 1$, in modo che risulti:

   $$d \cdot e - \varphi(n) \cdot x = 1$$

   Eseguiamo la divisione:

   $$\begin{aligned} 352 &= 8 \times 43 + 8 \\ 43 &= 5 \times 8 + 3 \\ 8 &= 2 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

   Quindi, ripercorrendo al contrario:

$$1 = 3 - 1 \times 2$$
$$1 = 3 - 1 \times (8 - 2 \times 3) = 3 - 8 + 2 \times 3 = 3 \times 3 - 8$$
$$1 = 3 \times 3 - 8 = 3(43 - 5 \times 8) = 3 \times 43 - 15 \times 8 - 8 = 3 \times 43 - 16 \times 8$$
$$1 = 3 \times 43 - 13 \times 8 = 3 \times 43 - 16(352 - 8 \times 43) = 3 \times 43 - 16 \times 352 + 128 \times 43$$
$$131 \times 43 - 16 \times 352 = 1$$
$$\rightarrow d = 131$$

Altrimenti, ricordando che $a^{-1} \bmod z = a^{\varphi(z)-1} \bmod z$, calcoliamo d come $d = e^{-1} \bmod \varphi(n)$:

$$d = e^{-1} \bmod \varphi(n) = e^{\varphi(\varphi(n))-1} \bmod \varphi(n)$$

dove $\varphi(\varphi(n)) = \varphi(352)$.

Sapendo che $352 = 2^5 \cdot 11$, calcoliamo $\varphi(352)$ usando i suoi fattori primi distinti.

Dato che ogni numero è esprimibile come combinazione dei suoi fattori primi p_i, ovvero $x = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_n^{a_n}$, la funzione totiente vale

$$\varphi(x) = x \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_n}\right)$$

che in questo caso è

$$\varphi(352) = 352 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{11}\right) =$$
$$= 352 \cdot \frac{1}{2} \cdot \frac{10}{11} = 160.$$

Quindi, tornando al calcolo di d:

$$d = e^{-1} \bmod \varphi(n) =$$
$$= e^{\varphi(\varphi(n))-1} \bmod \varphi(n) =$$
$$= e^{\varphi(352)-1} \bmod 352 =$$
$$= 43^{160-1} \bmod 352 =$$
$$= 43^{159} \bmod 352 = 131$$

il risultato $d = 131$ è identico a quello trovato in precedenza.

Ora proviamo a cifrare il numero 200, e poi a decifrare il risultato:

$$m = 200 \rightarrow c = m^e \bmod n = 200^{43} \bmod 391 = 174$$

$$c = 174 \rightarrow m = c^d \bmod n = 174^{131} \bmod 391 = 200$$

Strategia *square-and-multiply* per le potenze

Vogliamo calcolare $b^e \bmod m$. Possiamo utilizzare il seguente metodo:

1. Rappresentare e in binario e inizializzare il risultato r a $r = 1$
2. Scandire e_{bin} dal bit più significativo a quello meno significativo e, per ogni bit e_i:
   - $r = r^2 \bmod m$ (sempre)
   - se $e_i = 1$, calcolare anche $r = r \cdot b \bmod m$

Ad esempio, volendo calcolare $5^{13} \bmod 23$:

1. l'esponente è $13_{\text{dec}} = 1101_{\text{bin}}$

2. $r = 1$; per ogni bit:

   Bit più significativo uguale a 1, square and multiply:

   $$e_3 = 1 \to r = 1 \cdot 1 \bmod 23 = 1; r = 1 \cdot 5 \bmod 23 = 5$$

   Secondo bit più significativo uguale a 1, square and multiply:

   $$e_2 = 1 \to r = 5 \cdot 5 \bmod 23 = 2; r = 2 \cdot 5 \bmod 23 = 10$$

   Terzo bit più singificativo uguale a 0, square:

   $$e_1 = 0 \to r = 10 \cdot 10 \bmod 23 = 8$$

   Bit meno signficativo uguale a 1, square and multiply:

   $$e_0 = 1 \to r = 8 \cdot 8 \bmod 23 = 18; r = 18 \cdot 5 \bmod 23 = 21$$

Il risultato finale è dunque 21.

Velocizzazione dello *square-and-multiply* usando il teorema cinese del resto

Data la chiave privata

$$k_{\text{priv}} = \langle d, p, q, \varphi(n) \rangle$$

la decifratura avviene secondo la formula

$$m = c^{d \bmod \varphi(n)} \bmod n.$$

Possiamo calcolare

$$m_p = c^d \bmod p = c^{d \bmod (p-1)} \bmod p$$
$$m_q = c^d \bmod q = c^{d \bmod (q-1)} \bmod q$$

e ricombinare le due parti secondo le seguenti relazioni basate sul teorema cinese del resto:

$$m = c^{d \bmod \varphi(n)} \bmod n \Leftrightarrow \begin{cases} m = m_p \bmod p \\ m = m_q \bmod q \end{cases} \Leftrightarrow \begin{cases} m = c^{d \bmod \varphi(p)} \bmod p \\ m = c^{d \bmod \varphi(q)} \bmod q \end{cases}$$

così che

$$m = \left(q(q^{-1} \bmod p)m_p + p(p^{-1} \bmod q)m_q\right) \bmod n.$$

Ad esempio, supponiamo di voler decifrare il ciphertext creato nell'esempio RSA. Ricordiamo i parametri:

- $c = 174$, $m = 200$
- $k_{\text{pub}} = \langle e, n \rangle = \langle 43, 391 \rangle$
- $k_{\text{priv}} = \langle p, q, \varphi(n), d \rangle = \langle 17, 23, 352, 131 \rangle$

Calcoliamo ora m_p e m_q:

$$\begin{aligned} m_p = c^d \bmod p = c^{d \bmod (p-1)} \bmod p &= \\ = 174^{131 \bmod 16} \bmod 17 &= \\ = 174^3 \bmod 17 = 13 \end{aligned}$$

$$\begin{aligned} m_q = c^d \bmod q = c^{d \bmod (q-1)} \bmod q &= \\ = 174^{131 \bmod 22} \bmod 23 &= \\ = 174^{21} \bmod 23 = 16 \end{aligned}$$

Il plaintext m è dunque

$$m = \left(q(q^1 \bmod p)m_p + p(p^{-1} \bmod q)m_1\right) \bmod n =$$
$$= (23(23^{-1} \bmod 17) \cdot 13 + 17(17^{-1} \bmod 23) \cdot 16) \bmod 391$$

Ci servono $23^{-1} \bmod 17$ e $17^{-1} \bmod 23$. Usiamo la formula per gli inversi basata sulla funzione totiente di Eulero:

$$a^{-1} \bmod l = a^{\varphi(l)-1}$$

Per il 23:

$$23^{-1} \bmod 17 = 6^{-1} \bmod 17$$

Dato che 17 è un numero primo, vale $\varphi(p) = p - 1$:

$$\varphi(17) = 17 - 1) = 16$$

quindi

$$6^{-1} \bmod 17 = 6^{16-1} \bmod 17 = 6^{15} \bmod 17 = 3$$

(infatti $3 \cdot 6 \bmod 17 = 1$). Ora procediamo con $17^{-1} \bmod 23$. Sappiamo che, come prima, $\varphi(23) = 23 - 1 = 22$, quindi

$$17^{-1} \bmod 23 = 17^{22-1} \bmod 23 = 17^{21} \bmod 23 = 19$$

(infatti $19 \cdot 17 \bmod 23 = 1$).

Ora che abbiamo $p^{-1} = 19$ e $q^{-1} = 3$, riprendiamo i calcoli per trovare il plaintext:

$$m = \left(q(q^1 \bmod p)m_p + p(p^{-1} \bmod q)m_1\right) \bmod n =$$
$$= (23(23^{-1} \bmod 17) \cdot 13 + 17(17^{-1} \bmod 23) \cdot 16) \bmod 391 =$$
$$= (23 \cdot 3 \cdot 13 + 17 \cdot 19 \cdot 16) \bmod 391 = 200.$$

Il calcolo risulta corretto, dato che il risultato individuato corrisponde al plaintext originale $m = 200$.

Crittografia basata sul DLP

Diffie-Hellman

Sia dato un gruppo $G =< g >$ generato da un elemento generatore g, di ordine $n = |G|$.

Il gruppo può essere generato nel modo seguente:

1. scegliere due numeri primi p_1 e p_2
2. calcolare $p = 2p_1p_2 + 1$
3. trovare un sottogruppo di ordine p_1 calcolandone il generatore g:

   $$g = p_2^{\frac{p-1}{p_1}} \bmod p$$

   In alcuni casi questa formulazione non funziona, perché produce come risultato 1, numero inadatto a fungere da generatore.

   In tal caso vale la formula generica

$$g = \alpha^{\frac{p-1}{p_1}} \bmod p$$

con $\alpha \in \mathbb{Z}_p^*$, ovvero $1 < \alpha < p-1$. Diventa necessario procedere per tentativi, variando α fino a trovare un $g \neq 1$.

Lo scambio di chiavi Diffie-Hellman avviene secondo i seguenti passaggi:

1. Alice e Bob estraggono casualmente le loro chiavi private all'interno del campo, dunque con $0 < k_{\text{priv}} \leq n$:

$$k_{\text{priv,A}} \leftarrow \$(\mathbb{Z}_n)$$
$$k_{\text{priv,B}} \leftarrow \$(\mathbb{Z}_n)$$

2. Alice e Bob generano le loro chiavi pubbliche a partire dalle chiavi private e dal generatore del campo:

$$k_{\text{pub,A}} = g^{k_{\text{priv,A}}}$$
$$k_{\text{pub,B}} = g^{k_{\text{priv,B}}}$$

3. Alice e Bob si scambiano le chiavi pubbliche (in un messaggio firmato)
4. Alice e Bob ricavano la chiave di sessione:

$$k_{\text{AB}} = \left(k_{\text{pub,B}}\right)^{k_{\text{priv,A}}}$$
$$k_{\text{BA}} = \left(k_{\text{pub,A}}\right)^{k_{\text{priv,B}}}$$

Vale $k_{\text{BA}} = k_{\text{AB}}$ grazie alle proprietà del campo.

Esempio

Per la generazione del gruppo:

1. scegliamo $p_1 = 7$ e $p_2 = 11$
2. calcoliamo $p = 2p_1p_2 + 1$:

$$p = 2 \cdot 7 \cdot 11 + 1 = 155$$

3. troviamo il generatore del sottogruppo di ordine $n = p_1 = 7$:

$$\begin{aligned} g &= p_2^{\frac{p-1}{p_1}} \bmod p = \\ &= 11^{\frac{154}{7}} \bmod 155 = \\ &= 11^{22} \bmod 155 = 111 \end{aligned}$$

A questo punto possiamo procedere con lo scambio DH:

1. estrazione casuale delle chiavi private, comprese tra 1 e 154:

$$k_{\text{priv,A}} = 123$$
$$k_{\text{priv,B}} = 32$$

2. generazione delle chiavi pubbliche, con $k_{\text{priv}} = g^{k}_{\text{pub}}$:

$$k_{\text{pub,A}} = 111^{123} \bmod 155 = 66$$
$$k_{\text{pub,B}} = 111^{32} \bmod 155 = 76$$

3. scambio delle chiavi: Bob ottiene $k_{\text{pub,A}}$, Alice ottiene $k_{\text{pub,B}}$
4. calcolo della chiave di sessione:

$$k_{\text{AB}} = k_{\text{pub,B}}^{k_{\text{priv,A}}} = 76^{123} \bmod 155 = 16$$
$$\text{k\_BA} = k_{\text{pub,A}}^{k_{\text{priv,B}}} = 66^{32} \bmod 155 = 16$$

Se le due chiavi di sessione corrispondono ($k_{\text{BA}} = k_{\text{AB}}$), la procedura è da considerarsi corretta.

ElGamal

Chiavi

Il sistema è definito in un gruppo $G =< g >$ di dimensione $|G| = n$ e un suo elemento $s \in \mathbb{Z}_n$.

Chiave pubblica:

$$k_{\text{pub}} = \langle n, g, g^s \rangle$$

Chiave privata:

$$k_{\text{priv}} = \langle s \rangle$$

Creazione delle chiavi

Creazione delle chiavi:

1. scegliere un numero primo grande p; l'ordine del gruppo risultante è $n = p - 1$
2. trovare il generatore g del gruppo moltiplicativo modulo p. Questo significa che, per $1 < x < p$, $g^x \bmod p$ produce tutti gli elementi del gruppo (i numeri da 1 a n)
3. scegliere la chiave segreta, un qualsiasi s tale che $1 < s < p - 1$
4. calcolare $g^s \bmod p$

Cifratura e decifratura

Il messaggio m è un membro di G: $m \in G$

Cifratura:

1. scegliere l da $\mathbb{Z}_n^*$ (ovvero compreso tra 1 e n)
2. calcolare $\gamma = g^l$
3. calcolare $\delta = m \cdot (g^s)^l$

Il ciphertext è $\langle \gamma, \delta \rangle$

Decifratura:

$$m = \gamma^{n-s} \cdot \delta$$

Esempio di cifratura e decifratura

Creazione delle chiavi:

1. scegliere un numero primo, in questo caso $p = 23$, quindi il gruppo ha ordine $n = p - 1 = 22$
2. trovare il generatore g del gruppo moltiplicativo modulo p. Questo significa che, per $1 < x < p$, $g^x \bmod p$ produce tutti gli elementi del gruppo (i numeri da 1 a n). Possiamo scegliere $g = 5$ perché

$$5^1 \bmod 23 = 5$$
$$5^2 \bmod 23 = 2$$
$$5^3 \bmod 23 = 10$$
$$5^4 \bmod 23 = 4$$
$$5^5 \bmod 23 = 20$$
$$5^6 \bmod 23 = 8$$
$$5^7 \bmod 23 = 17$$
$$5^8 \bmod 23 = 16$$
$$5^9 \bmod 23 = 11$$
$$5^{10} \bmod 23 = 9$$
$$5^{11} \bmod 23 = 22$$
$$5^{11} \bmod 23 = 18$$
$$5^{13} \bmod 23 = 21$$
$$5^{14} \bmod 23 = 13$$
$$5^{15} \bmod 23 = 19$$
$$5^{16} \bmod 23 = 3$$
$$5^{17} \bmod 23 = 15$$
$$5^{18} \bmod 23 = 6$$
$$5^{19} \bmod 23 = 7$$
$$5^{20} \bmod 23 = 12$$
$$5^{21} \bmod 23 = 14$$
$$5^{22} \bmod 23 = 1$$

E questo produce tutti i numeri da 1 a 22.

3. scegliere la chiave segreta, un qualsiasi s tale che $1 < s < n$:

$$s = 6$$

4. calcolare $g^s \bmod n$:

$$5^6 \bmod 23 = 8$$

La chiave pubblica è dunque $\langle 22, 5, 8 \rangle$, mentre la chiave privata è $\langle 6 \rangle$.

Scegliamo di cifrare il numero $m = 13$.

1. prendiamo un l casuale da $\mathbb{Z}_n^*$, compreso tra 1 e $n - 1$:

$$l = 7$$

2. calcoliamo $\gamma = g^l$:

$$\gamma = 5^7 \bmod 23 = 17$$

3. calcoliamo $\delta = m \cdot (g^s)^l$:

$$\begin{aligned}\delta = \left(13 \cdot \left((5^6 \bmod 23)^7 \bmod 23\right)\right) \bmod 23 = \\ = (13 \cdot (8^7 \bmod 23)) \bmod 23 = \\ = (13 \cdot 12) \bmod 23 = \\ = 18\end{aligned}$$

Il ciphertext è dunque $\langle 17, 18 \rangle$. Per decifrare:

$$\begin{aligned}m = (\gamma^{n-s} \cdot \delta) \bmod 23 = \\ = ((17^{22-6} \bmod 23) \cdot 18) \bmod 23 = \\ = (2 \cdot 18) \bmod 23 = \\ = 13\end{aligned}$$

Firme
La creazione delle chiavi è identica a quella per la cifratura.

Per creare una firma, partendo da un messaggio m:

1. generare un l casuale compreso tra 1 e n
2. calcolare $\gamma = g^l$
3. dati $h(m)$ (l'hash del messaggio) e $h(\gamma)$ (l'hash di γ), calcolare

$$\delta = l^{-1} \cdot (h(m) - s \cdot h(\gamma)) \bmod n$$

La firma S corrisponde a $\langle \gamma, \delta \rangle$. Il messaggio firmato è $\langle m, S \rangle$.

Per verificare la firma:

1. calcolare $h(m)$ (l'hash del messaggio) e $h(\gamma)$ (l'hash di γ)
2. accettare la firma se:

$$(g^s)^{h(\gamma)} \cdot \gamma^\delta = g^{h(m)}$$

Esempio per la firma
Riutilizziamo le chiavi e il messaggio dell'esempio precedente:

$$k_{\text{priv}} = s = 6$$
$$k_{\text{pub}} = \langle n, g, g^s \rangle = \langle 22, 5, 8 \rangle$$

Assumiamo che la funzione hash corrisponda semplicemente alla versione modulo n del numero ($n = 22$).

1. scegliamo, come in precedenza, $l = 7$
2. calcoliamo $\gamma = g^l$:

$$\gamma = 5^7 \bmod 23 = 17$$

3. calcoliamo $\delta = l^{-1} \cdot (h(m) - s \cdot h(\gamma)) \bmod n$:

$$\begin{aligned} \delta = 19 \cdot (13 - 6 \cdot 17 \bmod 22) \bmod 22 = \\ = 19 \cdot (13 - 14) \bmod 22 = \\ = 19 \cdot (-1) \bmod 22 = \\ = 19 \cdot 21 \bmod 22 = \\ = 3 \end{aligned}$$

(ricordando che l'inverso l^{-1} è quel numero tale che $l^{-1} \cdot l \bmod p = 1$)

La firma è $S = \langle 17, 3 \rangle$. Verifichiamola, calcolando i due termini e controllando se corrispondono:

$$\begin{gathered} (g^s)^{h(\gamma)} \cdot \gamma^\delta = \\ = (8^{17} \bmod 23) \cdot (17^3 \bmod 23) \bmod 23 = \\ = 13 \cdot 14 \bmod 23 = \\ 13 \cdot 14 \bmod 23 = 21 \end{gathered}$$

$$g^{h(m)} = 5^{13} \bmod 23 = 21$$

La firma è dunque correttamente verificata.