Questo fascicolo contiene
un esempio di compito (esercizi).
Gli esercizi sono svolti. Ci sono
anche due domande facoltative:
cercate di rispondere da soli.
Questi esercizi verranno discussi
nella lezione di domani
Venerdì 23 maggio 2019

Crittografia 2018-19

Esempio di compito d'esame (esercizi)

Esercizio 1

A. è titolare di un crittosistema R.S.A. con $p=79$, $q=41$, $e=23$ (come al solito, p,q sono primi ed e è la chiave pubblica di cifratura).

Si domanda:

i) calcolare la "decryption-key" d di A.

ii) calcolare la "decryption-key" minima d_1 di A.

iii) B. cifra per A. il messaggio $M=7$: qual'è il cifrato che A. riceve?

Esercizio 2

B. è titolare di un crittosistema di El Gamal con

$(p,g,\beta) = (83,2,47) \longrightarrow$ chiave pubblica

$a=23 \longrightarrow$ chiave privata

(quindi $p=83$ è primo, 2 è radice primitiva mod 83 e $\beta = 47 \equiv g^a \equiv 2^{23} \pmod{83}$)

Si domanda

a) A. cifra per B. il messaggio $M=5$, con parametro di mascheratura $k=10$. Qual'è il cifrato che A. riceve?

b) B. firma per A. il messaggio in chiaro $M=7$, con parametro di mascheratura $k=13$. Qual'è la terna $(M,S')=(M,\gamma,\delta))$ che A. riceve?

Esercizio sul crittosistema R.S.A.

Svolgimento

A. è titolare di un crittosistema R.S.A. con $p=79$, $q=41$, $e=23$. (come al solito p, q sono primi ed $e=23$ è la chiave pubblica di cifratura).

Si domanda

i) calcolare la "decryption-key" d di A.

ii) calcolare la "decryption-key" minima d_1 di A.

iii) B. cifra per A. il messaggio $M=7$: qual'è il cifrato C che A. riceve?

Rispondiamo, come prima cosa, alla domanda i). Siccome $\varphi(n)=\varphi(p\cdot q)=(p-1)(q-1)=$
$=78\cdot 40=3120$, si tratta di risolvere la congruenza $ed\equiv 1 \pmod{\varphi(n)}$, per noi

$$23d\equiv 1 \pmod{3120}$$

Mediante l'algoritmo euclideo otteniamo

$3120 = 23\cdot 135 + (15)$
$23 = 15\cdot 1 + (8)$
$15 = 8\cdot 1 + (7)$
$8 = 7\cdot 1 + (1)$
$7 = 1\cdot 7 + 0$

da cui segue

$1 = 8-7 = 8-(15-8) = 2\cdot 8 - 15 =$
$= 2\cdot(23-15) - 15 = 2\cdot 23 - 3\cdot 15 =$
$= 2\cdot 23 - 3(3120 - 23\cdot 135)$
$= 23(407) - 3120(3)$

Si ha quindi $d = 407$.

2) $\boxed{d = 407}$

ii) Vediamo ora la "decryption-key" minima d_1.

Si ha $\lambda(n) = \frac{\varphi(n)}{(p-1, q-1)} = \frac{78 \cdot 40}{(78, 40)} = \frac{78 \cdot 40}{2} = 1560$.

Dobbiamo quindi risolvere la congruenza

3) $e d_1 \equiv 1 \pmod{\lambda(n)}$

che per noi diviene

4) $23 d_1 \equiv 1 \pmod{1560}$

$$1560 = 23 \cdot 67 + (19)$$
$$23 = 19 \cdot 1 + (4)$$
$$19 = 4 \cdot 4 + (3)$$
$$4 = 3 \cdot 1 + (1)$$

e quindi $1 = 4 - 3 = 4 - (19 - 4 \cdot 4) = 4 \cdot 19 =$

$$= (23 - 19) - 19 = 5 \cdot 23 - 6 \cdot 19 =$$
$$= 5 \cdot 23 - 6 (1560 - 23 \cdot 67) =$$
$$= 23 (5 + 6 \cdot 67) - 6 \cdot 1560$$
$$= 23 (5 + 402) - 6 \cdot 1560$$
$$= 23 \cdot 407 - 6 \cdot 1560$$

da cui segue $d_1 \equiv 407 \pmod{1560}$

e quindi

5) $\boxed{d_1 = 407}$

Quindi $d = d_1$ (lo si poteva prevedere, in questo caso: spiegate bene il perché (domanda facoltativa))^2

Cifriamo ora il messaggio $M = 7$. Si ha

$$6) \quad C \equiv M^e \pmod{n}$$

Per noi $n = 79 \cdot 41 = 3239$, $e = 23$, $M = 7$ e quindi la 6) diviene

$$7) \quad C \equiv 7^{23} \pmod{3239}$$

Si ha

$$7 \equiv 7 \pmod{3239}$$
$$7^2 \equiv 49$$
$$7^4 \equiv (49)^2 \equiv 2401 \equiv -838 \pmod{3239}$$
$$7^8 \equiv 702244 \equiv -619 \pmod{3239}$$
$$7^{16} \equiv 383161 \equiv 959 \pmod{3239}$$
$$7^{20} \equiv 7^{16} \cdot 7^4 \equiv 959 \cdot 2401 \equiv 2302559 \equiv 2869 \pmod{3239}$$
$$7^{22} \equiv 2869 \cdot 49 \equiv 140581 \equiv 1304 \pmod{3239}$$
$$7^{23} \equiv 1304 \cdot 7 \equiv 9128 \equiv 2650 \pmod{3239}$$

Quindi

$$8) \quad \boxed{C = 2650}$$

Veniamo ora all'esercizio sul crittosistema El Gamal. Le pagine che seguono contengono le soluzioni dei quesiti a) e b).

- Bob è titolare di un El Gamal con $(p, g, \beta) = (83, 2, 47)$, chiave pubblica

$a = 23$, chiave privata

(quindi $p = 83$ è primo, $g = 2$ è radice primitiva mod 83 e $\beta = 47 \equiv g^a \equiv 2^{23} \pmod{83}$)

a) Alice cifra per Bob il messaggio $M = 5$ con parametro di mascheramento $k = 10$. Qual'è il cifrato che Bob riceve?

Si tratta di calcolare

$$9) \quad \begin{cases} \gamma \equiv g^k \pmod p \\ \delta \equiv M \beta^k \pmod p \end{cases}$$

che per noi diviene

$$10) \quad \begin{cases} \gamma \equiv 2^{10} \pmod{83} \\ \delta \equiv 5 \cdot 47^{10} \pmod{83} \end{cases}$$

Si ha

$$11) \quad 2^{10} \equiv 1024 \equiv 28 \pmod{83}$$

e

$$47 \equiv 47 \pmod{83}$$
$$47^2 \equiv 47 \cdot 47 \equiv 2209 \equiv 51 \pmod{83}$$
$$47^4 \equiv 51^2 \equiv 2601 \equiv 28 \pmod{83}$$
$$47^8 \equiv (28)^2 \equiv 784 \equiv 37 \pmod{83}$$
$$47^8 \cdot 47^2 \equiv 37 \cdot 51 = 1887 \equiv 61 \pmod{83}$$

cioè

$$12) \quad 47^{10} \equiv 61 \pmod{83}$$

e quindi

13) $\delta \equiv 5 \cdot 47^{10} \equiv 5 \cdot 61 \equiv 305 \equiv 56 \pmod{83}$

Perciò Bob riceve (vedi 10), 11) e 13))

14) $C = (\gamma, \delta) = (28, 56)$

b) Bob firma il messaggio $M = 7$ con parametro di mascheratura $k = 13$. Qual'è la terna $(M, S) = (M, \gamma, \delta)$ che Alice riceve?

Rispondiamo: per firmare si calcolano

15) $\begin{cases} \gamma \equiv g^k \pmod{p} \\ \delta \equiv (M - a\gamma) k^{-1} \pmod{(p-1)} \end{cases}$

Calcoliamo k^{-1}, per noi la $k \cdot k^{-1} \equiv 1 \pmod{(p-1)}$ diviene

16) $13 \cdot k^{-1} \equiv 1 \pmod{82}$

$82 = 13 \cdot 6 + 4$
$13 = 4 \cdot 3 + 1$ e quindi $1 = 13 - 4 \cdot 3 =$
$= 13 - (82 - 13 \cdot 6) 3$
$= 19 \cdot 13 - 3 \cdot 82$

e perciò

17) $k^{-1} \equiv 19 \pmod{82}$

Inoltre, essendo $2^{10} \equiv 1024 \equiv 28 \pmod{83}$ (vedi prima)
si ha $2^{13} \equiv 2^{10} \cdot 2^3 \equiv 28 \cdot 8 \equiv 224 \equiv 58 \pmod{83}$

Quindi

18) $r \equiv g^k \pmod{p}$ per noi diviene

19) $r \equiv 2^{13} \equiv 58 \pmod{83}$

mentre

20) $s \equiv (M - ar)(k^{-1}) \bmod (p-1)$ diviene

21) $s \equiv (7 - 23 \cdot 58) \cdot 19 \equiv (7 - 23(-24)) \cdot 19 \equiv$
$\equiv (7 + 552) \cdot 19 \equiv 559 \cdot 19 \equiv 67 \cdot 19 \equiv 1273 \equiv$
$\equiv 43 \pmod{82}$

Dunque la firma di $M = 7$ è

$(M, S) = (M, (r, s)) = (7, (58, 43))$

Domanda facoltativa

Il matematico francese Pierre de Fermat (1601-1665) congetturò che i numeri della forma

1) $F_K = 2^{(2^K)} + 1$ (con $K = 0, 1, 2, 3, \ldots$)

fossero tutti primi. In effetti $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ lo sono. Nel 1732 Eulero scoprì che $F_5 = 2^{32} + 1 = (641)(6700417)$ è composto.

Osservate che

2) $641 = 640 + 1 = 5 \cdot 2^7 + 1$

da cui segue

$\rightarrow$ 3) $5 \cdot 2^7 \equiv -1 \pmod{641}$

e 4) $641 = 625 + 16 = 5^4 + 2^4$

da cui segue

$\rightarrow$ 5) $5^4 \equiv -2^4 \pmod{641}$

Partendo dalle congruenze 3) e 5) saprete dimostrare rapidamente il risultato di Eulero, cioè

6) $(641) \mid (2^{32} + 1)$?