Esercizi

a.a. 2013/14

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@dia.unisa.it

http://www.dia.unisa.it/professori/ads

Maggio 2014

Indice

- Cifratura simmetrica
- RSA
- Diffie-Hellman
- Funzioni hash
- MAC

Esercizio: cifratura simmetrica 1

Cifratura $E_a(x) = ax \bmod 26$

Si determini sotto quali condizioni sulla chiave a, la funzione di cifratura $E_a(\bullet)$ risulta univocamente decifrabile.

Si determini la dimensione dello spazio delle chiavi.

Esercizio: cifratura simmetrica 1

Cifratura $E_a(x) = ax \bmod 26$

Se $y = ax \bmod 26$

Allora $x = a^{-1}y \bmod 26$

Quindi le chiavi sono tutti gli a che hanno inverso mod 26

Esercizio: cifratura simmetrica 1

Cifratura $E_a(x) = ax \bmod 26$

Se $y = ax \bmod 26$

Allora $x = a^{-1}y \bmod 26$

Quindi le chiavi sono tutti gli a che hanno inverso mod 26
Hanno inverso tutti gli a con gcd(a,26)=1
Dato che 26=13•2, tali a sono in totale (13-1)(2-1)=12

Esercizio: cifratura simmetrica 1

Inversi

1•1=1 mod 26

3•9=1 mod 26

5•21=1 mod 26

7•15=1 mod 26

11•19=1 mod 26

17•23=1 mod 26

25•25=1 mod 26

Ovvero

1,3,5,7,9,11,15,
17,19,21,23,25

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Esercizio: cifratura simmetrica 1

Valori di a per cifratura unicamente decifrabile

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
NO	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a=1 →	1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
NO	2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
a=3 →	3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
NO	4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
a=5 →	5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
NO	6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
a=7 →	7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
NO	8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
a=9 →	9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
NO	10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
a=11 →	11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
NO	12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
NO	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
NO	14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
a=15 →	15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
NO	16	0	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
a=17 →	17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
NO	18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
a=19 →	19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
NO	20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
a=21 →	21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
NO	22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
a=23 →	23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
NO	24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
a=25 →	25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Esercizio: cifratura simmetrica 2

Cifratura $E_{a,b}(x) = ax+b \bmod 26$

Si determini sotto quali condizioni sulla chiave a, la funzione di cifratura $E_a(\bullet)$ risulta univocamente decifrabile.

Si determini la dimensione dello spazio delle chiavi (a,b).

Sia (a,b)=(7,3). Si determini la cifratura del messaggio CIAO.

Esercizio: RSA

Sia (n=35, e=11) la chiave RSA pubblica

- Calcolare la chiave privata mediante l'algoritmo esteso di Euclide.
- Calcolare la firma del messaggio m=8, mediante un algoritmo di esponenziazione modulare a scelta tra left-to-right e right-to-left.

Esercizio: RSA

Si consideri il seguente algoritmo per la scelta dei primi p e q per RSA:

```
p ← mumero primo di 2.048 bit, scelto a caso
q ← p
repeat
    q ← q+2
until q è dichiarato primo dal test di primalità
```

Cioè, p e q sono primi consecutivi.

Si analizzi la sicurezza del risultante schema RSA.

Esercizio: Diffie-Hellman

Chiarire se nello scambio di chiavi Diffie-Hellman è possibile utilizzare $p=17$, $g=2$ come parametri pubblici.

Esercizio: Funzioni hash

Sia h_1: $\{0,1\}^{2r} \rightarrow \{0,1\}^r$ una funzione hash che soddisfa la proprietà di sicurezza forte e sia h_2: $\{0,1\}^{4r} \rightarrow \{0,1\}^r$ una seconda funzione hash definita come segue: per ogni $x \in \{0,1\}^{4r}$, sia $x = x_1 \,||\, x_2$, dove $x_1, x_2 \in \{0,1\}^{2r}$ (il simbolo $||$ denota la concatenazione di due stringhe) e sia

$$h_2(x) = h_1(h_1(x_1)||h_1(x_2))$$

Provare che anche la funzione h_2 soddisfa la proprietà di sicurezza forte.

Esercizio: MAC

Si consideri la seguente funzione MAC valida per messaggi m di lunghezza arbitraria, costruita a partire dal cifrario simmetrico AES e dalla funzione MD5. Per un messaggio m, con chiave condivisa k, sia

$$MAC_k(m) = AES_{MD5(m)}(k).$$

Descrivere i parametri di funzionamento del MAC proposto e analizzarne la sicurezza, giustificando le risposta.

Domande?