Galeasso Federico 5L 2/12/2023

Esercitazione RSA

1. Generazione delle chiavi

p=5
q=13
N=p*q=5*13=65
V=(p-1)*(q-1)=(5-1)*(13-1)=48
Npri=11
Npub=(n*V+1)/Npri
Npub=(n*48+1)mod 11=0
n=8
Npub=(8*48+1)/11=35

Kpub(65,35)
Kpri(65,11)

Chiave pubblica di Galfrè: Kpub(15,13)

2. Cifratura del messaggio

Parola segreta scelta: panino

p	01110000
a	01100001
n	01101110
i	01101001
n	01101110
o	01101111

Messaggio in chiaro
01110000011000010110111001101001011011100110111

La sequenza di bit è divisa in blocchi di g bit, in modo che g sia il più piccolo numero tale che $2^g \geq 65$; in questo caso g = 7.

Divisione in blocchi di 7 bit:
0111000 0011000 0101101 1100110 1001011 0111001 0101111

Blocco	In decimale	Cifratura del blocco con chiave (15,13)	Blocco cifrato in decimale	Blocco cifrato in binario
0111000	56	$56^{13} \bmod 15$	11	0001011
0011000	24	$24^{13} \bmod 15$	9	0001001
0101101	45	$45^{13} \bmod 15$	0	0000000

1100110	102	$102^{13} \bmod 15$	12	0001100
1001011	75	$75^{13} \bmod 15$	0	0000000
0111001	57	$57^{13} \bmod 15$	12	0001100
0101111	47	$47^{13} \bmod 15$	2	0000010

Messaggio cifrato
000101100010010000000000110000000000011000000010

3. Decifratura del messaggio

Messaggio cifrato di Galfrè
111110 100111 001010 101010 000100 101010 001001 100101

Blocco	In decimale	Cifratura del blocco con chiave (65,11)	Blocco cifrato in decimale	Blocco cifrato in binario
111110	62	$62^{11} \bmod 65$	43	101011
100111	39	$39^{11} \bmod 65$	39	100111
001010	10	$10^{11} \bmod 65$	30	11110
101010	42	$42^{11} \bmod 65$	48	110000
000100	4	$4^{11} \bmod 65$	49	110001
101010	42	$42^{11} \bmod 65$	48	110000
001001	9	$9^{11} \bmod 65$	29	11101
100101	37	$37^{11} \bmod 65$	58	111010

10101110011111110110000110001110000111011111010

111010

Blocco decifrato

10101110	01111111	01100001	10001110	00011101	111010
®		a	□	#	