Esempio di applicazione dell'RSA

Alice deve inviare a Bob il proprio indirizzo, ma deve fare in modo che Lia (che controlla il canale di comunicazione) non ne venga a conoscenza.
A questo proposito Alice e Bob decidono di utilizzare l'algoritmo RSA per proteggere la loro comunicazione.

Mittente: Alice Destinatario: Bob

1. **Generazione delle chiavi**

Bob deve generare le chiavi di cifratura (k_{pub}) e decifratura (k_{pri}).

Scegliamo $p = 5$ e $q = 11$ (per semplicità prendiamo dei numeri piccoli)

$n = p \cdot q = 5 \cdot 11 = 55$
$V = (p - 1) \cdot (q - 1) = 4 \cdot 10 = 40$

Determiniamo N_{pri} che non abbia fattori comuni con V, quindi con 40.
Prendiamo ad esempio $N_{pri} = 7$.

Determiniamo N_{pub} tale che $[(N_{pri} \cdot N_{pub}) \pmod V] = 1$ che equivale a cercare un multiplo di V che soddisfi la relazione seguente $[(n \cdot V + 1) \pmod{N_{pri}}] = 0$ che mi permette di calcolare il valore di N_{pub} come $N_{pub}=(n \cdot V + 1)/N_{pri}$

Nel nostro caso:

$[(7 \cdot N_{pub}) \pmod{40}] = 1$

ossia $[(n \cdot 40 + 1) \pmod 7] = 0$

ossia $n \cdot 40 + 1 = 7 \cdot N_{pub}$ cioè $N_{pub} = (n \cdot 40 + 1)/7$

dove n è un qualunque numero intero positivo

Se prendiamo $n = 4$, allora $N_{pub} = 23$

La coppia di chiavi generata da Bob è quindi la seguente:

$K_{pub}(55,23)$ $K_{pri}(55,7)$

2. **Cifratura del messaggio**

Alice deve inviare il suo indirizzo a Bob; il messaggio è quindi: “via Roma”. Ogni lettera è tradotta in binario (per esempio in codice ASCII).

v	01110110
i	01101001
a	01100001
	00100000
R	01010010
o	01101111
m	01101101
a	01100001

Messaggio in chiaro

01110110011010010110000100100000010100100110111101101101011000 01

La sequenza di bit è divisa in blocchi di g bit, in modo che g sia il più piccolo numero tale che $2^g \geq 55$; in questo caso $g = 6$.

Divisione in blocchi di 6 bit:

011101 100110 100101 100001 001000 000101 001001 101111 011011 010110 000001

Poiché l’ultimo blocco in questo caso è di soli 4 bit (0001) aggiungiamo due zeri davanti (000001).

Blocco	In decimale	Cifratura del blocco con chiave (55,23)	Blocco cifrato in decimale	Blocco cifrato in binario
011101	29	$29^{23} \bmod 55$	24	011000
100110	38	$38^{23} \bmod 55$	37	100101
100101	37	$37^{23} \bmod 55$	53	110101
100001	33	$33^{23} \bmod 55$	22	010110
001000	8	$8^{23} \bmod 55$	17	010001
000101	5	$5^{23} \bmod 55$	15	001111
001001	9	$9^{23} \bmod 55$	14	001110
101111	47	$47^{23} \bmod 55$	38	100110
011011	27	$27^{23} \bmod 55$	48	110000
010110	22	$22^{23} \bmod 55$	33	100001
000001	1	$1^{23} \bmod 55$	1	000001

Messaggio cifrato

011000100101110101010110010001001111001110100110110000100001000001

3. **Decifratura del messaggio**

Messaggio cifrato

011000100101110101010110010001001111001110100110110000100001000001

Blocco cifrato in binario	Blocco cifrato in decimale	Decifratura del blocco con chiave (55,7)	Blocco decifrato in decimale	Blocco decifrato in binario
011000	24	$24^7 \bmod 55$	29	011101
100101	37	$37^7 \bmod 55$	38	100110
110101	53	$53^7 \bmod 55$	37	100101
010110	22	$22^7 \bmod 55$	33	100001
010001	17	$17^7 \bmod 55$	8	001000
001111	15	$15^7 \bmod 55$	5	000101
001110	14	$14^7 \bmod 55$	9	001001
100110	38	$38^7 \bmod 55$	47	101111
110000	48	$48^7 \bmod 55$	27	011011
100001	33	$33^7 \bmod 55$	22	010110
000001	1	$1^7 \bmod 55$	1	000001

Blocco decifrato

01110110	01101001	01100001	00100000	01010010	01101111	01101101	01100001
v	i	a		R	o	m	a

NOTA: Nell'ultimo ottetto, sono stati tolti 2 bit.