Un esempio pratico

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

K_1 CHIAVE PUBBLICA: $n=1189,\ a=747$

Il messaggio da cifrare è: $x=(374,0,652,0)$

SVOLGIMENTO:

1. Cerco i due numeri primi p e q tali che $n=p\cdot q$:

$$1189=29\cdot 41$$

(in questo caso abbiamo scelto un numero n piccolo,
in modo tale da trovare facilmente la sua fattorizzazione)

2. Calcolo $\varphi(n)=(p-1)\cdot(q-1)=28\cdot 40=1120$

3. Trovo b dall'identità di Bézout, verificando al tempo stesso che valga $M.C.D.(a,\varphi(n))=1$

$$1120=747\cdot 1+373 \ \Rightarrow\ 373=(1,0)+(0,1)\cdot(-1)=(1,-1)$$

$$747=373\cdot 2+1 \ \Rightarrow\ 1=(0,1)+(1,-1)\cdot(-2)=(0,1)+(-2,2)=(-2,3)$$

cioè vale $M.C.D.(a,\varphi(n))=1$ e inoltre dall'identità $1=1120\cdot(-2)+747\cdot(3)$ segue che $b=3$

4. Usando l'algoritmo 'Square and Multiply' decifro ogni singolo numero del messaggio:

- $374^3\equiv\ ?\ \ mod\ 1189$

  $b=3$ in codice binario è (11) per cui avremo XQX, cioè, partendo da 1, faremo una moltiplicazione per 374 - un elevamento al quadrato - una moltiplicazione per 374:

$$X:\ 1\cdot 374=374\ \ mod\ 1189$$
$$Q:\ 374^2=139876\equiv 763\ \ mod\ 1189$$
$$X:\ 763\cdot 374=285362\equiv 2\ \ mod\ 1189$$

  quindi la prima lettera del messaggio è: $2\ \rightarrow\ C$

- $0^3\equiv 0\ \ mod\ 1189$ quindi la seconda lettera del messaggio è: $0\ \rightarrow\ A$

- $652^3\equiv\ ?\ \ mod\ 1189$

  $b=3$ in codice binario è (11) per cui avremo XQX, cioè, partendo da 1, faremo una moltiplicazione per 652 - un elevamento al quadrato - una moltiplicazione per 652:

$$X:\ 1\cdot 652 = 652 \mod 1189$$
$$Q:\ 652^2 = 425104 \equiv 631 \mod 1189$$
$$X:\ 631\cdot 652 = 411412 \equiv 18 \mod 1189$$

quindi la terza lettera del messaggio è: $18 \rightarrow S$

- $0^3 \equiv 0 \mod 1189$ quindi l'ultima lettera del messaggio è: $0 \rightarrow A$

5. Il nostro messaggio decifrato è quindi: $x = (C, A, S, A)$, cioè la parola 'CASA'