un applicazione : la crittografia.

Sia M un messaggio.
Il mittente usa una funzione (algoritmo) che trasforma M in C e manda C
Il ricevente usa una funzione che trasforma C in M. Le funzioni dipendono da una chiave (password). La sicurezza è basata sulla chiave non sull'algoritmo.

$f(k) : M \longrightarrow C$ dove k è la chiave per codificare
$g(\ell) : C \longrightarrow M$ dove ℓ è la chiave per decodificare.

Simmetrica : $k = \ell$ o almeno "facile" riportare tra k e ℓ

esempio : cassaforte con una chiave.

esempio: Cesare:

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

$f : p \longmapsto p+3 \pmod{26}$ cioè $A \mapsto D$, $E \mapsto H$, $\vdots$, $X \to A$

per decodificare : $g : q \longmapsto q-3 \pmod{26}$

FDSLWR?

esempio: una variazione della crittografia di Cesare.

Siano $c, r \in \mathbb{Z}$ con $0 \le r < 26$ e $\mathrm{mcd}(c, 26) = 1$
cioè c è invertibile modulo 26.

$f(r,c) : p \longmapsto cp + r \pmod{26}$

$g(r,c) : q \longmapsto \ldots$ (esercizio).

Si osservi che c deve essere invertibile modulo 26
altrimenti $f(r,c)$ non è una bigezione

Esempio: $f(0,3) : p \to 3p \pmod{26}$ cioè
$A \to A$, $B \to D$, $C \to G$, ...

Non sono molto buone: si può fare statistica sulle parole.

asimmetrica : "crittografia a chiave pubblica"

Il mittente usa f e una chiave e, fornitti dal ricevente, per trasformare M in C. Il ricevente usa un altra chiave d per trasformare C in M. Il rapporto tra e e d è "difficile" da risolvere.

$f(e) : \mathcal{M} \longrightarrow \mathcal{C}$ $\qquad$ f, g, e sono pubblici

$g(d) : \mathcal{C} \longrightarrow \mathcal{M}$ $\qquad$ d è segreto.

Esempio: l'algoritmo RSA (R. Rivest, A. Shamir, L. Adleman, MIT 1977)

Siano p e q due numeri primi. Sia $n = p \cdot q$

Siano e e d due interi con $ed \equiv 1 \pmod{(p-1)(q-1)}$.

<u>Oss</u> Sia $A \in \mathbb{Z}$. Allora $A^{ed} \equiv A \pmod p$ e $A^{ed} \equiv A \pmod q$.

Dim: $ed = 1 + h(p-1)(q-1)$, per certo $h \in \mathbb{Z}$.

Se $p \mid A$ allora $A \equiv 0 \pmod p$ e $A^{ed} \equiv 0 \pmod p$ quindi $A^{ed} \equiv A \pmod p$

se $p \nmid A$ allora $A^{ed} = A^{1+h(p-1)(q-1)} = A \cdot A^{h(p-1)(q-1)} = A \cdot \left(A^{(p-1)}\right)^{h(q-1)}$

ma $A^{p-1} \equiv 1 \pmod p$, quindi $A^{ed} \equiv A \pmod p$.

In ogni caso abbiamo $A^{ed} \equiv A \pmod p$.

Simile $A^{ed} \equiv A \pmod q$.

Sia $A \in \mathbb{Z}$ con $0 \le A < n$. Allora $\begin{cases} A^{ed} \equiv A \pmod p \\ A^{ed} \equiv A \pmod q \end{cases}$

Segue che A^{ed} è una soluzione del sistema $\begin{cases} x \equiv A \pmod p \\ x \equiv A \pmod q \end{cases}$

Ma anche A è una soluzione di questo sistema.

Dal teorema cinese dei resti segue che $A^{ed} \equiv A \pmod{pq}$

cioè $A^{ed} \equiv A \pmod n$. Ma $A < n$, quindi $A^{ed} \pmod n = A$.

Pubblico n, e

Privato d

Sia $0 \le M < n$ $\qquad$ codifica: $M \longrightarrow M^e \pmod n$

decodifica $C \longrightarrow C^d \pmod n$

Allora $M \longrightarrow M^e \pmod n \longrightarrow C^d \pmod n = M$

codifica $C = M^e \pmod n$ $\qquad$ decodifica $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M \pmod n$

<u>Sicurezza</u> Se conosco p e q (per esempio se posso fattorizzare n) allora posso calcolare d con l'algoritmo di Euclide, perché d è un inverso di e modulo $(p-1)(q-1)$.

Esempio

$n = 143$ $\quad p = 13$ $\quad q = 11$, allora $(p-1)(q-1) = 120$

$e = 7$ $\quad 120 = 7 \cdot 17 + 1$ $\quad 1 = 120 - 7 \cdot 17$

$1 = 120 + 7 \cdot (-17)$ $\quad -17$ è un inverso di 7 modulo 120

$-17 \pmod{120} = 103$

Pubblichiamo $n = 143$, $e = 7$

Segreto $d = 103$.

Prendiamo il messaggio 80

codificare: $80^7 \pmod{143}$ $\quad 80^7$ è un numero grande

facciamo così: $80^2 \equiv 6400 \equiv 108 \pmod{143}$

$80^3 \equiv 108 \cdot 80 \equiv 60 \pmod{143}$

$80^6 \equiv 60 \cdot 60 \equiv 25 \pmod{143}$

$80^7 = 25 \cdot 80 \equiv 141 \pmod{143}$

Il messaggio codificato è 141

decodificare 141 dobbiamo calcolare $141^{103} \pmod{143}$ ----

fare come prima è troppo lento, facciamo così: prima 103 in base 2

$103 = 2 \cdot 51 + 1$

$51 = 2 \cdot 25 + 1$

$25 = 2 \cdot 12 + 1$

$12 = 2 \cdot 6 + 0$

$6 = 2 \cdot 3 + 0$

$3 = 2 \cdot 1 + 1$

$1 = 2 \cdot 0 + 1$

$103 = (1100111)_2$

$= 2^6 + 2^5 + 2^2 + 2 + 1$

$= 64 + 32 + 4 + 2 + 1$

Quindi $(141)^{103} = (141)^{64} \cdot (141)^{32} \cdot (141)^4 \cdot (141)^2 \cdot (141)$

Adesso calcoliamo le potenze di 141 modulo 143

$(141)^2 \equiv 4 \pmod{143}$

$(141)^4 = 16 \pmod{143}$

$(141)^8 \equiv 16^2 \equiv 113 \pmod{143}$

$(141)^{16} \equiv 113^2 \equiv 42 \pmod{143}$

$(141)^{32} \equiv 42^2 \equiv 48 \pmod{143}$

$(141)^{64} \equiv 48^2 \equiv 16 \pmod{143}$

Quindi $(141)^{103} \equiv 16 \cdot 48 \cdot 16 \cdot 4 \cdot 141 \pmod{143}$

$\equiv 80 \pmod{143}$

Quindi il messaggio decodificato è 80

Si può fare la decodificazione anche in un modo più veloce

Sono in possesso di 11 e 13, cioè p e q

vale che $M \equiv (141)^{103} \pmod{11}$ e $M \equiv (141)^{103} \bmod 13$ e $0 \le M < 143$

$141 = 11 \cdot 12 + 9$ quindi $11 \nmid 141$ posso applicare il piccolo teorema di Fermat

$103 = 10 \cdot 10 + 3$ quindi $(141)^{103} \equiv 9^{103} \pmod{11}$

$\equiv (9^{10})^{10} \cdot 9^3 \pmod{11}$ $(9^{10} \equiv 1 \pmod{11})$

$\equiv 9^3 \pmod{11}$

$\equiv 3 \pmod{11}$.

$141 = 13 \cdot 10 + 11$ quindi $13 \nmid 141$ posso applicare il piccolo teorema di Fermat

$103 = 12 \cdot 8 + 7$ quindi $(141)^{103} \equiv 11^{103} \pmod{13}$

$\equiv (11^{12})^8 \cdot 11^7 \pmod{13}$ $(11^{12} \equiv 1 \pmod{13})$

$\equiv 11^7 \pmod{13}$

$\equiv 2 \pmod{13}$

Quindi M è una soluzione di $\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 2 \pmod{13} \end{cases}$

Il teorema cinese di resti dice $x \equiv 80 \pmod{143}$. cioè $M = 80$.

Nel esempio ogni messaggio deve essere un numero < 143.

Come mandare un testo segreto? Per esempio una lettera di amore: Ti amo!

t		i		spazio		a		m		o		!		← ASCII
0101	0100	0100	1001	0010	0000	0100	0001	0100	1101	0100	1111	0010	0001	
5	4	4	9	2	0	4	1	4	13	4	15	2	1	

Vediamo il codice ASCII come una lunga bit string. La spezziamo in blocchi di lunghezza 4. (in pratica di lunghezza 512, cioè di 64 caratteri). Ogni blocco vediamo come un numero in base 2. Trovo una sequenza di numeri tra 0 e 15 (e quindi < 143). Nel nostro esempio la sequenza è

5, 4, 4, 9, 2, 0, 4, 1, 4, 13, 4, 15, 2, 1 codifichiamo ogni numero con RSA

Troviamo 47, 82, 82, 48, 128, 0, 82, 1, 82, 117, 82, 80, 128, 1

Questo viene mandato al ricevente, Lui/Lei decodifica, scrive i numeri in base 2, incolla i bit string e poi divide in blocchi di lunghezza 8 e prende il carattere ascii corrispondente.

Sicurezza: non si sa un modo di fattorizzare n velocemente se n è "grande", dove i primi sono "bit length" 512. Ma non è detto che non esiste un metodo veloce!! solo che finora non lo sappiamo.

Esempio: Firma elettronica. Sono l'unico che possa dare M e M^d tutti possono controllare che M^d corrisponde ad M usando la mia chiave pubblico (perché $M^{de} \equiv M \pmod{n}$).