proprietà di $\mathbb{Z}_n$

$n = pq$

problema di RSA è dato e con $MCD(e, \varphi(n)) = 1$
e $c \in \mathbb{Z}_n$ calcolare $c^{\frac{1}{e}}$

oss: $\boxed{MCD(e, \varphi(n)) = 1}$ $\Rightarrow$ ogni elemento $c \in \mathbb{Z}_n^*$ ammette esattamente una radice e-esima.

→ che ne ammette almeno una lo sappiamo.
calcoliamo d tale che $ed + k\varphi(n) = 1$

$$(c^d)^e = c$$

→ che sia esattamente una, osserviamo che
se

$$m^e = x = m'^e \Rightarrow (m^{-1}m')^e = 1$$

$\Rightarrow o(m^{-1}m') \mid e$ ma $o(m^{-1}m') \mid \varphi(n)$

e $MCD(e, \varphi(n)) = 1 \Rightarrow$

$o(m^{-1}m') = 1 \Rightarrow m^{-1}m' = 1 \Rightarrow m = m'$ □

N.B Se $MCD(e, \varphi(n)) > 1 \Rightarrow$ di radici ce ne possono essere tante (anche troppe).

MOSTRIAMO CHE IN $\mathbb{Z}_n$ con $n = pq$ ($p, q > 2$) CI SONO 4 radici quadrate per ogni elemento quadrato.

Supponiamo che $c = x^2$ e sia ε tale che $\varepsilon^2 = 1$

$$\Rightarrow (x\varepsilon)^2 = c$$

Mostriamo che 1 ammette 4 radici quadrate.

$\bar{x} = 1$

$\begin{cases} x = 1 \mod p \\ x = 1 \mod q \end{cases}$ $\qquad$ $\begin{cases} x = 1 \mod p \\ x = -1 \mod q \end{cases}$ $\to \bar{x} = \varepsilon$

$\bar{x} = -\varepsilon$ $\qquad$ $\begin{cases} x = -1 \mod p \\ x = 1 \mod q \end{cases}$ $\qquad$ $\begin{cases} x = -1 \mod p \\ x = -1 \mod q \end{cases}$ $\to \bar{x} = -1$

in tutti e 4 i casi $\begin{cases} x^2 = 1 \mod p \\ x^2 = 1 \mod q \end{cases} \to x^2 = 1 \mod pq$

<u>oss</u>: Saper calcolare tutte le radici quadrate in $\mathbb{Z}_n$ implica saper fattorizzare n

perché per ogni elemento quadrato in $\mathbb{Z}_n$

$x = c^2$ $\quad$ noi abbiamo 2 coppie di
$c^2 \neq 0$ $\quad$ radici $\pm c$ $\quad$ $\pm \varepsilon c$

scriviamo $x - x = 0 = (c^2 - (\varepsilon c)^2) =$

$= (c - \varepsilon c)(c + \varepsilon c)$ $\quad$ con $\varepsilon c \neq \pm 1$

$= c^2 (1 - \varepsilon)(1 + \varepsilon) = 0$ in $\mathbb{Z}_n$

questo significa che $pq = n \mid c^2 (1-\varepsilon)(1+\varepsilon)$

ma allora visto che p e q sono primi

$p \mid c^2$ oppure $p \mid (1-\varepsilon)$ oppure $p \mid (1+\varepsilon)$

e notiamo che q non divide il medesimo fattore di p
perché altrimenti: $pq \mid c^2 \Rightarrow c^2 = 0$ 4

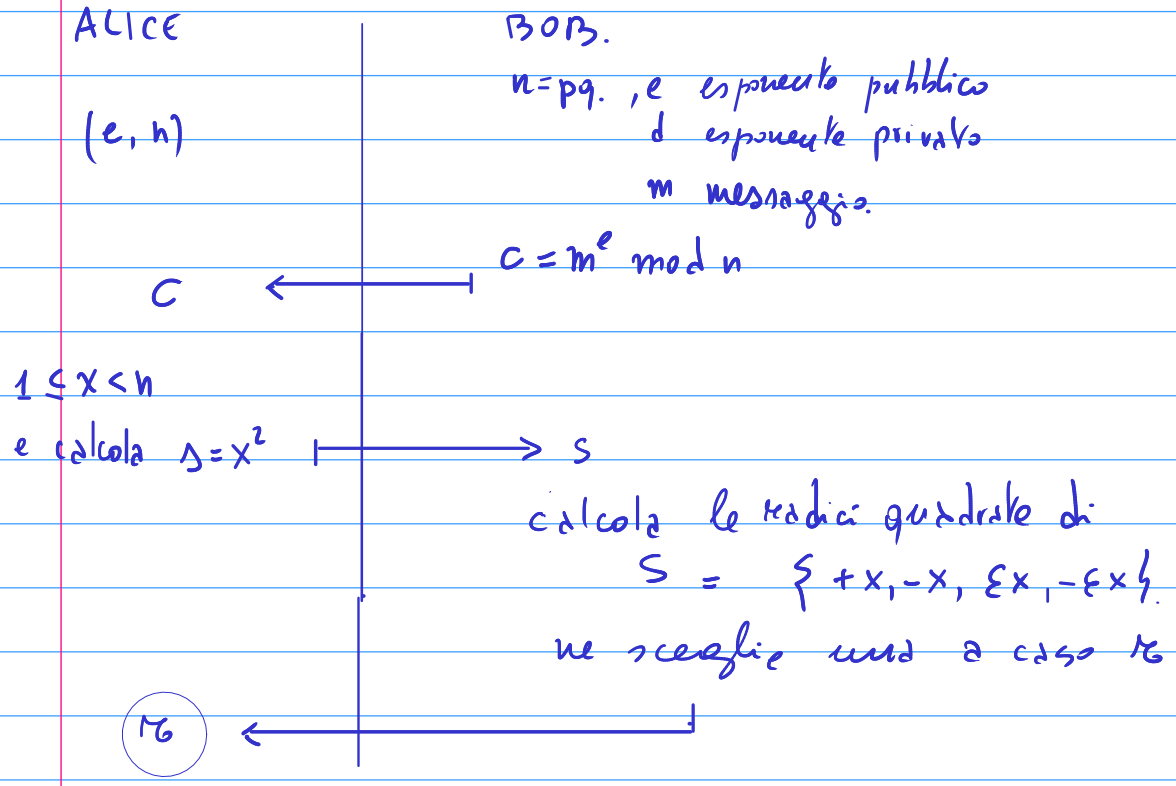
$pq \mid (1-\varepsilon) \Rightarrow 1-\varepsilon = 0 \Rightarrow \varepsilon = 1$ ✓

$pq \mid (1+\varepsilon) \Rightarrow 1+\varepsilon = 0 \Rightarrow \varepsilon = -1$ ✓

→ CALCOLIAMO $\{MCD(n, 1-\varepsilon), MCD(n, 1+\varepsilon)\} = \{p, q\}$

⇒ ABBIAMO FATTORIZZATO n

OBLIVIOUS TRANSFER.



1) $r = \pm x$ → alice non può fare nulla di nuovo

$(x+x)(x-x) = 0 \mod n$

2) $r = \pm \varepsilon x \neq \pm x$

⇒ calcola $(x+r)(x-r) = 0$

e deduce che

$\{p, q\} = \{MCD(x+r, n), MCD(x-r, n)\}$

ricava la fattorizzazione di n

→ calcola $\varphi(n) = (p-1)(q-1)$

calcola $ed + k\varphi(n) = 1$

calcola $c^d \mod n = m$

→ CON PROBABILITÀ $\frac{1}{2}$ ALICE HA RICEVUTO (e decodificato) m.

1) ALL-OR-NOTHING

2) DISTRIBUZIONE DI ELEMENTI CIFRATI DA BOB SENZA CHE BOB SAPPIA QUALI SONO →

ALICE

contributo A come seq. di BIT

C_A

$C_A^{(i)}$ $i = 1 \dots n$

codifica bit per bit

$d_A = (d_A^{(i)})$

BOB

contributo → seq. di bit B

C_B

$C_B^{(j)}$ $j = 1 \dots n$

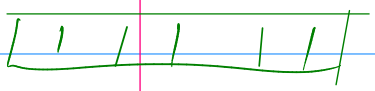
codifica bit per bit

$d_B = (d_B^{(j)})$

d_A →

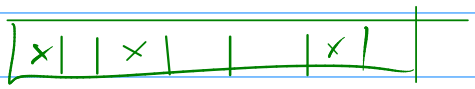
← d_B

ALICE chiede a BOB metà dei bit di d_B $(o\text{-}T\ \frac{1}{2})$



$\frac{1}{2} + \frac{1}{4} + \frac{1}{8}$

BOB chiede ad ALICE metà dei bit di d_A $(o\text{-}T\ \frac{1}{2})$



$\frac{1}{2} + \frac{1}{4} + \frac{1}{8}$

$\frac{1}{2^e}$

$OT\ \frac{1}{2}$ → ALICE MANDA A BOB UN MESSAGGIO SCELTO FRA 2 NON SA QUALE.

ALICE BOB

RSA $\rightsquigarrow n = pq$, e, d

$ed + k\varphi(n) = 1$

$(e, n) \longmapsto (e, n)$

m_1, m_2 messaggi

Genera 2 nonce x_1, x_2 $\longmapsto$ x_1, x_2

sceglie k NONCE $b \in \{1, 2\}$.

$v \longleftarrow v = (x_b + k^e) \bmod n$

$k_1 = (v - x_1)^d \bmod n$

$k_2 = (v - x_2)^d \bmod n$

uno dei due è k

$m_1' = m_1 + k_1$

$m_2' = m_2 + k_2$ $\longmapsto$ m_1', m_2'

se $k = k_1 \Rightarrow m_1 = m_1' - k$

ma $m_2' - k \neq m_2$

viceversa se $k = k_2$

→ BOB decodifica solo uno dei 2 messaggi possibili

→ ALICE non sa quale dei due.

OSS Tutto ha un senso a patto che le codifiche di m_1 ed m_2 siano indistinguibili.

(NON) SICUREZZA SEMANTICA DI RSA

1) RSA è deterministico → date le chiavi un messaggio si codifica in uno ed un solo modo (≠ ELGAMAL)

$2^3 = 8$ 101 010

SICUREZZA SEMANTICA IND-CPA

indistinguishability under chosen plaintext

ALICE BOB

$n = pq$, $ed \equiv k\varphi(n) = 1$

n ← n

m_1, m_2 messaggi → m_1, m_2

$c_i = m_i^e \bmod n$ $i = 1,2$

$j \in \{1,2\}$

c_j ← c_j

ALICE deve indovinare j ovvero di che messaggio c_j è codifica.

$m^e < n \Rightarrow m^e$ ha la stessa parità di m / caso banale

Simbolo di Jacobi-Legendre

→ ∃ una funzione calcolabile su m_i e su c_j e che è costante a meno della codifica

Simbolo di Legendre. Sia a un intero e p un primo dispari

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{se } p \mid a \\ 1 & \text{se } a = c^2 \bmod p \\ -1 & \text{se non esiste } c \text{ tale che } a = c^2 \bmod p. \end{cases}$$

si vede che $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$

infatti $a^{p-1} \bmod p = 1 \Rightarrow a^{\frac{p-1}{2}} = \pm 1$
se $p \nmid a$

in particolare se a è un quadrato $\Rightarrow a^{\frac{p-1}{2}} = +1$.

Infatti sia $\eta \in \mathbb{Z}_p^*$ tale che $\langle \eta \rangle = \mathbb{Z}_p^*$

$\Rightarrow$ I quadrati in $\mathbb{Z}_p^*$ sono elementi che si scrivono come $(\eta^2)^t$ ma allora

$$\left[(\eta^2)^t\right]^{\frac{p-1}{2}} = (\eta^{p-1})^t = 1 \text{ e quindi } \left(\frac{a}{p}\right) =$$

$$= a^{\frac{p-1}{2}} = \eta^{p-1} = 1$$

un non quadrato è del tipo (η^{2k+1})

$$(\eta^{2k+1})^{\frac{p-1}{2}} = \eta^{k(p-1)} \cdot \eta^{\frac{p-1}{2}}$$

$\eta^{k(p-1)} = 1$

ma $\eta^{\frac{p-1}{2}}$ ha ordine 2 perché $o(\eta) = p-1$

$$\Rightarrow \eta^{\frac{p-1}{2}} = -1 = \left(\frac{a}{p}\right)$$

Simbolo di Jacobi

Sia $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n}$ la fattorizzazione di n in primi ed $a \in \mathbb{Z}$

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{a_1} \left(\frac{a}{p_2}\right)^{a_2} \cdot \ldots \cdot \left(\frac{a}{p_n}\right)^{a_n}$$

simbolo di Jacobi — Simboli di Legendre

Oss RSA $n = pq$ m messaggio

e chiave pubblica è dispari perché $\varphi(n)$ è pari.

$c = m^e$

$$\left(\frac{c}{n}\right) = \left(\frac{c}{pq}\right) = \left(\frac{m^e}{pq}\right) = \left(\frac{m^e}{p}\right)\left(\frac{m^e}{q}\right) =$$

$$= \left(\frac{m}{p}\right)^e \left(\frac{m}{q}\right)^e = \left(\frac{m}{p}\right)\left(\frac{m}{q}\right) = \left(\frac{m}{n}\right)$$

e è dispari

perché se m è quadrato elevato a qualcosa e resta quadrato. se m è non quadrato

$\Rightarrow$ m elevato ad un esp. pari è quadrato ed elevato ad esp dispari è non quadrato.

Il simbolo di Jacobi del resto cifrato coincide col simbolo di Jacobi del resto in chiaro.

ALICE sceglie 2 messaggi con simboli di Jacobi differenti (a patto di poter calcolare il simbolo di Jacobi).

$$m_1 \rightarrow \left(\frac{m_1}{n}\right) = +1$$

$$m_2 \rightarrow \left(\frac{m_2}{n}\right) = -1$$

$c_i \leftarrow$ riceve

calcola $\left(\frac{c_i}{n}\right)$ $\begin{cases} = 1 \Rightarrow m_1 \\ = -1 \Rightarrow m_2 \end{cases}$

Vedremo che $\left(\frac{a}{n}\right)$ si può calcolare in modo molto rapido senza fattorizzare n