Università degli Studi di Cagliari
Corso di Laurea in Matematica

RSA e firma digitale

Mara Manca

Relatore: prof. Andrea Loi

Anno Accademico 2015-2016

Sommario

1. Crittologia
2. RSA
3. Matematica dietro la crittografia

Cos’è la crittologia?

La parola *crittologia* deriva dal greco *kryptòs*, che significa "nascosto".

Cos'è la crittologia?

La parola *crittologia* deriva dal greco *kryptòs*, che significa "nascosto".

Problema Alice vuole inviare un messaggio a Bob, impedendo a Eva, l'antagonista, di conoscere il contenuto del messaggio.

Cos'è la crittologia?

La parola *crittologia* deriva dal greco *kryptòs*, che significa "nascosto".

Problema Alice vuole inviare un messaggio a Bob, impedendo a Eva, l'antagonista, di conoscere il contenuto del messaggio.

Soluzione Alice invia una versione distorta del messaggio a Bob, che è l'unico in grado di ripristinare il messaggio in modo legittimo. In altre parole, Alice crittografa il messaggio (testo cifrato), lo invia a Bob, che a sua volta decodifica il messaggio (testo in chiaro).

Cos'è la crittologia?

La parola *crittologia* deriva dal greco *kryptòs*, che significa "nascosto".

Problema Alice vuole inviare un messaggio a Bob, impedendo a Eva, l'antagonista, di conoscere il contenuto del messaggio.

Soluzione Alice invia una versione distorta del messaggio a Bob, che è l'unico in grado di ripristinare il messaggio in modo legittimo. In altre parole, Alice crittografa il messaggio (testo cifrato), lo invia a Bob, che a sua volta decodifica il messaggio (testo in chiaro).

Chiave: parametro utilizzato per la cifratura o la decifratura decifrazione, permette di passare dal testo in chiaro al testo cifrato, e viceversa.

Cos'è la crittologia?

La crittologia può essere divisa in due categorie:

Cos'è la crittologia?

La crittologia può essere divisa in due categorie:
crittografia: si occupa della progettazione dei crittosistemi.

Cos'è la crittologia?

La crittologia può essere divisa in due categorie:
crittografia: si occupa della progettazione dei crittosistemi.
crittoanalisi: si occupa dell'attacco ai cifrari, ad esempio di come trovare la natura della chiave che è stata utilizzata.

Cos’è la crittologia?

La crittologia può essere divisa in due categorie:
crittografia: si occupa della progettazione dei crittosistemi.
crittoanalisi: si occupa dell’attacco ai cifrari, ad esempio di come trovare la natura della chiave che è stata utilizzata.

Cifrari simmetrici: la stessa chiave è utilizzata sia per la cifratura che per la decifrazione

Cos'è la crittologia?

La crittologia può essere divisa in due categorie:
crittografia: si occupa della progettazione dei crittosistemi.
crittoanalisi: si occupa dell'attacco ai cifrari, ad esempio di come trovare la natura della chiave che è stata utilizzata.

Cifrari simmetrici: la stessa chiave è utilizzata sia per la cifratura che per la decifrazione

Cifrari asimmetrici o a chiave pubblica: ogni utilizzatore del crittosistema possiede una chiave che è costituita da due parti: una pubblica e una privata.

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

- un insieme M di potenziali messaggi (sia testi in chiaro che testi cifrati);

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

- un insieme M di potenziali messaggi (sia testi in chiaro che testi cifrati);
- un insieme K di chiavi possibili;

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

- un insieme M di potenziali messaggi (sia testi in chiaro che testi cifrati);
- un insieme K di chiavi possibili;
- Per ogni k∈K esistono le funzioni invertibili

$$E_k : M \to M \qquad\qquad D_k : M \to M$$

tali che:

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

- un insieme M di potenziali messaggi (sia testi in chiaro che testi cifrati);
- un insieme K di chiavi possibili;
- Per ogni k∈K esistono le funzioni invertibili

$$E_k : M \to M \qquad D_k : M \to M$$

tali che:

1. $\forall k \in K$, $\exists k' \in K$ tale che $D_{k'}$ è l'inversa di E_k;

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

- un insieme M di potenziali messaggi (sia testi in chiaro che testi cifrati);
- un insieme K di chiavi possibili;
- Per ogni k∈K esistono le funzioni invertibili

$$E_k : M \to M \qquad D_k : M \to M$$

tali che:

1. $\forall k \in K$, $\exists k' \in K$ tale che $D_{k'}$ è l'inversa di E_k;
2. $\forall k \in K$ e $\forall m \in M$, $E_k(m) = c$ e $D_{k'}(c) = m$ sono facilmente calcolabili;

Crittosistema asimmetrico

Formalmente un crittosistema a chiave pubblica è costituito da:

- un insieme M di potenziali messaggi (sia testi in chiaro che testi cifrati);
- un insieme K di chiavi possibili;
- Per ogni k∈K esistono le funzioni invertibili

$$E_k : M \to M \qquad\qquad D_k : M \to M$$

tali che:

1. $\forall k \in K$, $\exists k' \in K$ tale che $D_{k'}$ è l'inversa di E_k;
2. $\forall k \in K$ e $\forall m \in M$, $E_k(m) = c$ e $D_{k'}(c) = m$ sono facilmente calcolabili;
3. per quasi tutti i $k \in$ K, non è computazionalmente possibile trovare $D_{k'}$, data E_k.

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;
3. Alice sceglie un *esponente di cifratura* $e \in \mathbb{Z}_s = \{0, \ldots, s-1\}$ tale che $MCD(e, s) = 1$;

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;
3. Alice sceglie un *esponente di cifratura* $e \in \mathbb{Z}_s = \{0, \dots, s-1\}$ tale che $MCD(e, s) = 1$;
4. Alice calcola d in modo che $de \equiv 1 \pmod{s}$;

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;
3. Alice sceglie un *esponente di cifratura* $e \in \mathbb{Z}_s = \{0, \dots, s-1\}$ tale che $MCD(e, s) = 1$;
4. Alice calcola d in modo che $de \equiv 1 \pmod s$;
5. Alice rende pubblici *(n,e)* (chiave pubblica), e tiene segreti *(p,q,d)* (chiave segreta);

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;
3. Alice sceglie un *esponente di cifratura* $e \in \mathbb{Z}_s = \{0, \dots, s-1\}$ tale che $MCD(e, s) = 1$;
4. Alice calcola d in modo che $de \equiv 1 \pmod s$;
5. Alice rende pubblici *(n,e)* (chiave pubblica), e tiene segreti *(p,q,d)* (chiave segreta);
6. Bob codifica il messaggio come una sequenza di interi $m_1, \dots, m_k$ tali che $1 \leq m_i < n-1 \ \forall i$.

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;
3. Alice sceglie un *esponente di cifratura* $e \in \mathbb{Z}_s = \{0, \ldots, s-1\}$ tale che $MCD(e, s) = 1$;
4. Alice calcola d in modo che $de \equiv 1 \pmod{s}$;
5. Alice rende pubblici *(n,e)* (chiave pubblica), e tiene segreti *(p,q,d)* (chiave segreta);
6. Bob codifica il messaggio come una sequenza di interi $m_1, \ldots, m_k$ tali che $1 \leq m_i < n-1 \ \forall i$.
   La sequenza $c_1, \ldots, c_k$ che rappresenta il testo cifrato, si trova calcolando $c_i \equiv m_i^e \pmod{n} \ \forall i = 1, \ldots, k$.
   Quindi Bob, invia questa sequenza ad Alice.

RSA

Supponiamo che Bob voglia mandare un messaggio ad Alice:

1. Alice sceglie due numeri primi grandi p e q tali che $p \neq q$;
2. Alice calcola $n = pq$ e $s = (p-1)(q-1)$;
3. Alice sceglie un *esponente di cifratura* $e \in \mathbb{Z}_s = \{0, \dots, s-1\}$ tale che $MCD(e, s) = 1$;
4. Alice calcola d in modo che $de \equiv 1 \pmod{s}$;
5. Alice rende pubblici *(n,e)* (chiave pubblica), e tiene segreti *(p,q,d)* (chiave segreta);
6. Bob codifica il messaggio come una sequenza di interi $m_1, \dots, m_k$ tali che $1 \leq m_i < n-1 \ \forall i$.
   La sequenza $c_1, \dots, c_k$ che rappresenta il testo cifrato, si trova calcolando $c_i \equiv m_i^e \pmod{n} \ \forall i = 1, \dots, k$.
   Quindi Bob, invia questa sequenza ad Alice.
7. Alice decifra il messaggio calcolando $m_i \equiv c_i^d \pmod{n} \ \forall i = 1, \dots, k$.

RSA

Teorema

Per ogni $i = 1, \ldots, k \;\; c_i^d \equiv m_i \pmod n$.

RSA

Teorema

Per ogni $i = 1, \ldots, k \;\; c_i^d \equiv m_i \;\; (mod\, n)$.

Definizione

Sia n$\geq$1 un intero e sia $\phi(n)$ il numero di elementi in $\mathbb{Z}_n = \{0, \ldots, n-1\}$ che sono relativamente primi con n.
La funzione ϕ definita in questo modo, è chiamata *funzione di Eulero*.

RSA

Teorema

Per ogni $i = 1, \ldots, k \;\; c_i^d \equiv m_i \pmod n$.

Definizione

Sia n$\geq$1 un intero e sia $\phi(n)$ il numero di elementi in $\mathbb{Z}_n = \{0, \ldots, n-1\}$ che sono relativamente primi con n.
La funzione ϕ definita in questo modo, è chiamata *funzione di Eulero*.

Teorema (Teorema di Eulero- Fermat)

Se a e n sono due interi relativamente primi, allora

$$a^{\phi(n)} \equiv 1 \pmod n$$

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod{n} \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod{n} \tag{1}$$

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod{n} \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod{n} \tag{1}$$

Ma $ed \equiv 1 \pmod{s}$, ciò significa che $s \mid ed - 1$.

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod{n} \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod{n} \tag{1}$$

Ma $ed \equiv 1 \pmod{s}$, ciò significa che $s \mid ed - 1$. Quindi, esiste un intero t tale che $st = ed - 1$.

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod{n} \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod{n} \tag{1}$$

Ma $ed \equiv 1 \pmod{s}$, ciò significa che $s \mid ed - 1$. Quindi, esiste un intero t tale che $st = ed - 1$.
Inoltre, $s = (p-1)(q-1) = \phi(pq) = \phi(n)$.

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod n \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod n \tag{1}$$

Ma $ed \equiv 1 \pmod s$, ciò significa che $s \mid ed - 1$. Quindi, esiste un intero t tale che $st = ed - 1$.
Inoltre, $s = (p-1)(q-1) = \phi(pq) = \phi(n)$.
Allora, $ed = st + 1 = \phi(n)t + 1$ e si ha

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod n \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod n \tag{1}$$

Ma $ed \equiv 1 \pmod s$, ciò significa che $s \mid ed - 1$. Quindi, esiste un intero t tale che $st = ed - 1$.
Inoltre, $s = (p-1)(q-1) = \phi(pq) = \phi(n)$.
Allora, $ed = st + 1 = \phi(n)t + 1$ e si ha

$$m_i^{ed} = m_i^{\phi(n)t+1} = \left(m_i^{\phi(n)}\right)^t m_i \tag{2}$$

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod n \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod n \tag{1}$$

Ma $ed \equiv 1 \pmod s$, ciò significa che $s \mid ed - 1$. Quindi, esiste un intero t tale che $st = ed - 1$.
Inoltre, $s = (p-1)(q-1) = \phi(pq) = \phi(n)$.
Allora, $ed = st + 1 = \phi(n)t + 1$ e si ha

$$m_i^{ed} = m_i^{\phi(n)t+1} = \left(m_i^{\phi(n)}\right)^t m_i \tag{2}$$

Avendo scelto m_i piccolo, $MCD(m_i, n) = 1$ quindi $m_i^{\phi(n)} \equiv 1 \pmod n$ grazie al teorema di Eulero-Fermat.

Dimostrazione teorema

$$c_i \equiv m_i^e \pmod n \quad \Rightarrow \quad c_i^d \equiv m_i^{ed} \pmod n \tag{1}$$

Ma $ed \equiv 1 \pmod s$, ciò significa che $s \mid ed - 1$. Quindi, esiste un intero t tale che $st = ed - 1$.
Inoltre, $s = (p-1)(q-1) = \phi(pq) = \phi(n)$.
Allora, $ed = st + 1 = \phi(n)t + 1$ e si ha

$$m_i^{ed} = m_i^{\phi(n)t+1} = \left(m_i^{\phi(n)}\right)^t m_i \tag{2}$$

Avendo scelto m_i piccolo, $MCD(m_i, n) = 1$ quindi $m_i^{\phi(n)} \equiv 1 \pmod n$ grazie al teorema di Eulero-Fermat. Dalle equazioni (1) e (2) otteniamo

$$c_i^d \equiv m_i^{ed} \equiv \left(m_i^{\phi(n)}\right)^t m_i \equiv (1)^t m_i \equiv m_i \pmod n \tag{3}$$

come enunciato.

Esempio

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è ’cat’.

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è 'cat'.
Per convenzione, numeriamo le lettere secondo lo schema

$$a \leftrightarrow 01, b \leftrightarrow 02, \ldots, z \leftrightarrow 26.$$

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è 'cat'.
Per convenzione, numeriamo le lettere secondo lo schema

$$a \leftrightarrow 01, b \leftrightarrow 02, \ldots, z \leftrightarrow 26.$$

Il messaggio risulta dunque: m= 30120.

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è 'cat'.
Per convenzione, numeriamo le lettere secondo lo schema

$$a \leftrightarrow 01, b \leftrightarrow 02, \ldots, z \leftrightarrow 26.$$

Il messaggio risulta dunque: m= 30120.
Il testo che Bob deve cifrare è molto corto, quindi sceglie di non dividere la parola che costituirà così un unico blocco.

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è 'cat'.
Per convenzione, numeriamo le lettere secondo lo schema

$$a \leftrightarrow 01, b \leftrightarrow 02, \ldots, z \leftrightarrow 26.$$

Il messaggio risulta dunque: m= 30120.
Il testo che Bob deve cifrare è molto corto, quindi sceglie di non dividere la parola che costituirà così un unico blocco.
Bob calcola $c \equiv m^e \equiv 30120^{9007} \equiv 113535859035722866 \pmod{n}$ e invia c ad Alice.

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è 'cat'.
Per convenzione, numeriamo le lettere secondo lo schema

$$a \leftrightarrow 01, b \leftrightarrow 02, \dots, z \leftrightarrow 26.$$

Il messaggio risulta dunque: m= 30120.
Il testo che Bob deve cifrare è molto corto, quindi sceglie di non dividere la parola che costituirà così un unico blocco.
Bob calcola $c \equiv m^e \equiv 30120^{9007} \equiv 113535859035722866 \pmod n$ e invia c ad Alice.
Alice, conoscendo p e q, calcola d in modo che $ed \equiv 1 \pmod s$; ottenendo d=116402471153538991

Esempio

Alice sceglie p=885320963 e q=238855417 primi e calcola n=211463707796206571 ed e=9007.
Alice manda a Bob la coppia (n, e) che rappresenta la chiave pubblica.
Il messaggio da cifrare è 'cat'.
Per convenzione, numeriamo le lettere secondo lo schema

$$a \leftrightarrow 01, b \leftrightarrow 02, \dots, z \leftrightarrow 26.$$

Il messaggio risulta dunque: m= 30120.
Il testo che Bob deve cifrare è molto corto, quindi sceglie di non dividere la parola che costituirà così un unico blocco.
Bob calcola $c \equiv m^e \equiv 30120^{9007} \equiv 113535859035722866 \pmod{n}$ e invia c ad Alice.
Alice, conoscendo p e q, calcola d in modo che $ed \equiv 1 \pmod{s}$; ottenendo d=116402471153538991
Infine Alice calcola
$c^d = 113535859035722866^{116402471153538991} \equiv 30120 \pmod{n}$; ottenendo il messaggio originale.

Sicurezza RSA

Teorema

Sia n=pq il prodotto di due primi p e q diversi tra loro.
Allora p e q sono le radici dell'equazione

$$x^2 - (n - \phi(n) + 1)x + n = 0$$

Teoremi

Teorema (Eulero- Fermat)

Se a e n sono due interi relativamente primi, allora

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Per provare il teorema di Eulero- Fermat, abbiamo necessità del seguente lemma.

Lemma

Siano x *e* y *interi tali che* $x \not\equiv y \pmod{n}$. *Se* $MCD(a, b) = 1$ *allora,* $ax \not\equiv ay \pmod{n}$.

Dimostrazione.

(Lemma) Supponiamo che $ax \equiv ay \pmod n$.
$MCD(a, b) = 1$ allora l'inverso moltiplicativo a^{-1} di a esiste.
Moltiplichiamo entrambi i membri per a^{-1}

$$a^{-1}ax \equiv a^{-1}ay \pmod n \iff x \equiv y \pmod n$$

che contraddice le ipotesi del teorema. $\square$

Dimostrazione.

(Teorema di Eulero-Fermat) Nell'insieme $\mathbb{Z}_n = \{0, \ldots, n-1\}$ troviamo $\phi(n)$ elementi relativamente primi con n. Indichiamo questi elementi con

$$x_1, \ldots, x_{\phi(n)} \tag{4}$$

Se $i \neq j \quad allora \quad x_i \not\equiv x_j \pmod n$. Poniamo

$$y_i = ax_i \pmod n \quad per \quad i = 1, \ldots, \phi(n)$$

e troviamo

$$y_1, \ldots, y_{\phi(n)} \tag{5}$$

elementi di $\mathbb{Z}_n$. Osserviamo che $MCD(x_i, n) = 1 \quad \forall\, i = 1, \ldots, \phi(n)$ (per definizione di $\phi(n)$), allora

$$MCD(y_i, n) = 1 \quad \forall\, i = 1, \ldots, \phi(n)$$

$$y_i \not\equiv y_j \pmod n \quad se \quad i \neq j$$

Dimostrazione.

Perciò $y_1, \ldots, y_{\phi(n)}$ è un elenco di elementi che sono tutti relativamente primi con n. Ciascun y_i in (5) compare esattamente una volta in (4) e ogni x_i compare solo una volta nell'elenco (5), allora

$$x_1 \cdots x_{\phi(n)} \equiv y_1 \cdots y_{\phi(n)} \pmod n \tag{6}$$

Dal momento che $y_i = ax_i \pmod n \quad \forall \quad i = 1, \ldots, \phi(n)$ allora,

$$y_1 \cdots y_{\phi(n)} \equiv ax_1 \cdots ax_{\phi(n)} \equiv a^{\phi(n)} x_1 \cdots x_{\phi(n)} \pmod n \tag{7}$$

Uguagliando le ultime due equazioni troviamo

$$a^{\phi(n)} x_1 \cdots x_{\phi(n)} \equiv x_1 \cdots x_{\phi(n)} \pmod n \tag{8}$$

Ogni x_i è relativamente primo con n, quindi, esistono i loro inversi moltiplicativi modulo n. Moltiplicando entrambi i membri per ciascun inverso, si ottiene il risultato $a^{\phi(n)} = 1 \pmod n$. □