Introduzione alla Crittografia

Progetto Lauree Scientifiche

Liceo Scientifico "N. Tron", 6 febbraio 2006

Riassunto

- Dato $n > 1$, la *funzione di Eulero* $\varphi(n)$ è il numero di elementi $< n$ e coprimi con n.

Riassunto

- Dato $n > 1$, la *funzione di Eulero* $\varphi(n)$ è il numero di elementi $< n$ e coprimi con n. Il numero di elementi invertibili in $\mathbb{Z}_n$ è esattamente $\varphi(n)$.

Riassunto

- Dato $n > 1$, la *funzione di Eulero* $\varphi(n)$ è il numero di elementi $< n$ e coprimi con n. Il numero di elementi invertibili in $\mathbb{Z}_n$ è esattamente $\varphi(n)$.
- Se p è primo $\varphi(p) = p - 1$.

Riassunto

- Dato $n > 1$, la *funzione di Eulero* $\varphi(n)$ è il numero di elementi $< n$ e coprimi con n. Il numero di elementi invertibili in $\mathbb{Z}_n$ è esattamente $\varphi(n)$.
- Se p è primo $\varphi(p) = p - 1$.
- Se $n = pq$, $\varphi(n) = (p-1)(q-1)$

Riassunto

- Dato $n > 1$, la *funzione di Eulero* $\varphi(n)$ è il numero di elementi $< n$ e coprimi con n. Il numero di elementi invertibili in $\mathbb{Z}_n$ è esattamente $\varphi(n)$.
- Se p è primo $\varphi(p) = p - 1$.
- Se $n = pq$, $\varphi(n) = (p-1)(q-1)$

Piccolo Teorema di Fermat

Teorema: *Se p è un numero primo, allora per ogni $a \in \mathbb{Z}$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Piccolo Teorema di Fermat

Teorema: *Se p è un numero primo, allora per ogni $a \in \mathbb{Z}$, $a \neq 0$, si ha*

$$a^{p-1} \equiv 1 \mod p$$

Corollario: *Sia $n = pq$ con p e q primi distinti, e sia e un intero tale che $(e, \varphi(n)) = 1$. Allora la funzione $f(x) = x^e$ è invertibile in $\mathbb{Z}_n$, e la sua inversa è data da $f^{-1}(x) = x^d$, dove $ed \equiv 1 \mod \varphi(n)$.*

- L'utente A sceglie in modo casuale due primi p e q distinti e molto grandi (circa 300 cifre decimali) e calcola $n = pq$;

- L'utente A sceglie in modo casuale due primi p e q distinti e molto grandi (circa 300 cifre decimali) e calcola $n = pq$;
- calcola $\varphi(n) = (p-1)(q-1)$;

- L'utente A sceglie in modo casuale due primi p e q distinti e molto grandi (circa 300 cifre decimali) e calcola $n = pq$;
- calcola $\varphi(n) = (p-1)(q-1)$;
- sceglie in modo casuale un intero e compreso tra 1 e $\varphi(n)$ e coprimo con $\varphi(n)$. In altre parole, sceglie casualmente un elemento invertibile in $\mathbb{Z}_{\varphi(n)}$;

- L'utente A sceglie in modo casuale due primi p e q distinti e molto grandi (circa 300 cifre decimali) e calcola $n = pq$;
- calcola $\varphi(n) = (p-1)(q-1)$;
- sceglie in modo casuale un intero e compreso tra 1 e $\varphi(n)$ e coprimo con $\varphi(n)$. In altre parole, sceglie casualmente un elemento invertibile in $\mathbb{Z}_{\varphi(n)}$;
- calcola $d \equiv e^{-1} \mod \varphi(n)$.

- L'utente A sceglie in modo casuale due primi p e q distinti e molto grandi (circa 300 cifre decimali) e calcola $n = pq$;
- calcola $\varphi(n) = (p-1)(q-1)$;
- sceglie in modo casuale un intero e compreso tra 1 e $\varphi(n)$ e coprimo con $\varphi(n)$. In altre parole, sceglie casualmente un elemento invertibile in $\mathbb{Z}_{\varphi(n)}$;
- calcola $d \equiv e^{-1} \mod \varphi(n)$. Conoscendo p e q, è facile calcolare d: basta prima calcolare $\varphi(n)$ e poi usare l'algoritmo di Euclide esteso per il calcolo dell'inverso di e;

- L'utente A sceglie in modo casuale due primi p e q distinti e molto grandi (circa 300 cifre decimali) e calcola $n = pq$;
- calcola $\varphi(n) = (p-1)(q-1)$;
- sceglie in modo casuale un intero e compreso tra 1 e $\varphi(n)$ e coprimo con $\varphi(n)$. In altre parole, sceglie casualmente un elemento invertibile in $\mathbb{Z}_{\varphi(n)}$;
- calcola $d \equiv e^{-1} \mod \varphi(n)$. Conoscendo p e q, è facile calcolare d: basta prima calcolare $\varphi(n)$ e poi usare l'algoritmo di Euclide esteso per il calcolo dell'inverso di e;
- rende pubblica la coppia (n, e), che è detta *chiave pubblica* di A, e tiene segreto d, che è detta *chiave privata* di A.

Dal Corollario al Piccolo Teorema di Fermat, segue che:

- La chiave pubblica (n, e) individua la funzione invertibile $f: \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = x^e \mod n$;

Dal Corollario al Piccolo Teorema di Fermat, segue che:

- La chiave pubblica (n, e) individua la funzione invertibile $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = x^e \mod n$;
- La chiave privata d individua la funzione inversa $f^{-1}\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f^{-1}(x) = x^d \mod n$.

Dal Corollario al Piccolo Teorema di Fermat, segue che:

- La chiave pubblica (n, e) individua la funzione invertibile $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = x^e \mod n$;
- La chiave privata d individua la funzione inversa $f^{-1}\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f^{-1}(x) = x^d \mod n$.
- $f^{-1}(f(x)) \equiv x \mod n$ per ogni intero x.

Dal Corollario al Piccolo Teorema di Fermat, segue che:

- La chiave pubblica (n, e) individua la funzione invertibile $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = x^e \mod n$;
- La chiave privata d individua la funzione inversa $f^{-1}\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f^{-1}(x) = x^d \mod n$.
- $f^{-1}(f(x)) \equiv x \mod n$ per ogni intero x.

In altre parole, la terna (n, e, d) individua la *chiave di cifratura* $x^e \mod n$ e la *chiave di decifratura* $x^d \mod n$

- Se B vuole mandare un messaggio P all'utente A, deve

- Se B vuole mandare un messaggio P all'utente A, deve
  - assicurarsi che $P < n$, in modo che P possa essere considerato un elemento di $\mathbb{Z}_n$;

- Se B vuole mandare un messaggio P all'utente A, deve
  - assicurarsi che $P < n$, in modo che P possa essere considerato un elemento di $\mathbb{Z}_n$;
  - cacolare e spedire $P^e \mod n$.

- Se B vuole mandare un messaggio P all'utente A, deve
  - assicurarsi che $P < n$, in modo che P possa essere considerato un elemento di $\mathbb{Z}_n$;
  - cacolare e spedire $P^e \mod n$.
- Se A vuole decifrare il messaggio ricevuto, deve

- Se B vuole mandare un messaggio P all'utente A, deve
  - assicurarsi che $P < n$, in modo che P possa essere considerato un elemento di $\mathbb{Z}_n$;
  - cacolare e spedire $P^e \mod n$.
- Se A vuole decifrare il messaggio ricevuto, deve
  - calcolare $(P^e)^d \mod n$;

- Se B vuole mandare un messaggio P all'utente A, deve
  - assicurarsi che $P < n$, in modo che P possa essere considerato un elemento di $\mathbb{Z}_n$;
  - cacolare e spedire $P^e \mod n$.
- Se A vuole decifrare il messaggio ricevuto, deve
  - calcolare $(P^e)^d \mod n$;
  - poichè sappiamo che $P^{ed} \equiv P \mod n$, A è in grado di ottenere esattamente P.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Chiave pubblica di A: $(35, 11)$.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Chiave pubblica di A: $(35, 11)$. Chiave privata di A: 13.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Chiave pubblica di A: $(35, 11)$. Chiave privata di A: 13.

B vuole mandare a A il messaggio $P = 4$:

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Chiave pubblica di A: $(35, 11)$. Chiave privata di A: 13.

B vuole mandare a A il messaggio $P = 4$:
B calcola $4^{11} = 4194304$ e $4194304 \mod 35 = 9$.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Chiave pubblica di A: $(35, 11)$. Chiave privata di A: 13.

B vuole mandare a A il messaggio $P = 4$:
B calcola $4^{11} = 4194304$ e $4194304 \mod 35 = 9$.

B spedisce 9.

Esempio

A sceglie come primi $p = 5$, $q = 7$; quindi $n = 35$ e $\varphi(n) = 24$.
Inoltre A sceglie $e = 11$, coprimo con 24 e calcola $d = 13$.

Chiave pubblica di A: $(35, 11)$. Chiave privata di A: 13.

B vuole mandare a A il messaggio $P = 4$:
B calcola $4^{11} = 4194304$ e $4194304 \mod 35 = 9$.

B spedisce 9.

A calcola $9^{13} = 2541865828329$ e $2541865828329 \mod 35 = 4$.

Esempio

Siano $p = 7$ e $q = 13$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) =$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d =$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d = 29$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d = 29$

chiave pubblica $(91, 5)$, chiave privata 29

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d = 29$

chiave pubblica $(91, 5)$, chiave privata 29

Vogliamo codificare $P = 7$:

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d = 29$

chiave pubblica $(91, 5)$, chiave privata 29

Vogliamo codificare $P = 7$: $C = 63$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d = 29$

chiave pubblica $(91, 5)$, chiave privata 29

Vogliamo codificare $P = 7$: $C = 63$

Vogliamo decodificare $C = 80$

Esempio

Siano $p = 7$ e $q = 13$ quindi $n = 91$;

calcoliamo $\varphi(n) = 72$

scegliamo $e = 5$ e calcoliamo $d = 29$

chiave pubblica $(91, 5)$, chiave privata 29

Vogliamo codificare $P = 7$: $C = 63$

Vogliamo decodificare $C = 80$: $P = 19$

Problemi

- Il metodo è sicuro?

Problemi

- Il metodo è sicuro?
- Come si convertono lettere in numeri, o meglio, lettere in elementi di $\mathbb{Z}_n$?

Problemi

- Il metodo è sicuro?
- Come si convertono lettere in numeri, o meglio, lettere in elementi di $\mathbb{Z}_n$?
- Fissata la chiave pubblica (n, e), di quante lettere possono essere composti i messaggi da cifrare?

Sicurezza

La sicurezza del metodo si basa:

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e).

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e). Algoritmi di primalità.

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e). Algoritmi di primalità.
- nota la chiave pubblica (n, e), per ottenere la chiave privata bisogna conoscere $\varphi(n)$. Per conoscere $\varphi(n)$ bisogna conoscere la fattorizzazione $n = pq$.

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e). Algoritmi di primalità.
- nota la chiave pubblica (n, e), per ottenere la chiave privata bisogna conoscere $\varphi(n)$. Per conoscere $\varphi(n)$ bisogna conoscere la fattorizzazione $n = pq$. Questo può essere estremamente difficile. Algoritmi di fattorizzazione.

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e). Algoritmi di primalità.
- nota la chiave pubblica (n, e), per ottenere la chiave privata bisogna conoscere $\varphi(n)$. Per conoscere $\varphi(n)$ bisogna conoscere la fattorizzazione $n = pq$. Questo può essere estremamente difficile. Algoritmi di fattorizzazione. Numeri RSA.

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e). Algoritmi di primalità.
- nota la chiave pubblica (n, e), per ottenere la chiave privata bisogna conoscere $\varphi(n)$. Per conoscere $\varphi(n)$ bisogna conoscere la fattorizzazione $n = pq$. Questo può essere estremamente difficile. Algoritmi di fattorizzazione. Numeri RSA.
- bisogna costruire dei primi p e q in modo oppurtuno affinchè la fattorizzazione di n non sia calcolabile in tempi ragionevoli.

Sicurezza

La sicurezza del metodo si basa:

- relativa facilità di costruire primi molto grandi, e quindi di costruire chiavi pubbliche del tipo (n, e). Algoritmi di primalità.
- nota la chiave pubblica (n, e), per ottenere la chiave privata bisogna conoscere $\varphi(n)$. Per conoscere $\varphi(n)$ bisogna conoscere la fattorizzazione $n = pq$. Questo può essere estremamente difficile. Algoritmi di fattorizzazione. Numeri RSA.
- bisogna costruire dei primi p e q in modo oppurtuno affinchè la fattorizzazione di n non sia calcolabile in tempi ragionevoli. Per fare ciò p e q devono essere molto grandi (circa 300 cifre) e non vicini tra loro.

Conversione di parole in numeri

Fissiamo un alfabeto di 30 caratteri: "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" "," "." ";" " ' " " "

Conversione di parole in numeri

Fissiamo un alfabeto di 30 caratteri: "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" "," "." ";" " ' " " "

Supponiamo di voler cifrare la parole PARMA.

Conversione di parole in numeri

Fissiamo un alfabeto di 30 caratteri: "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" "," "." ";" " ' " " "

Supponiamo di voler cifrare la parole PARMA.

A tale parola facciamo corrispondere il numero:

$$x = 15 \cdot 30^4 + 0 \cdot 30^3 + 17 \cdot 30^2 + 12 \cdot 30^1 + 0 \cdot 30^0$$

In questa scrittura x è espresso in base 30-aria; nella usuale scrittura decimale, $x = 12165660$.

In base 30, x ha esattamente 5 cifre, in base decimale ne ha 8.

Il numero che vogliamo trasmettere, corrispondente alla parola PARMA, è 12165660. Dobbiamo quindi scegliere $n = pq$ tale che $n > 12165660$.

Lunghezza dei messaggi cifrabili

Fissata una chiave pubblica (n, e), qual è la lunghezza massima di un messaggio che possiamo cifrare con tale chiave?

Lunghezza dei messaggi cifrabili

Fissata una chiave pubblica (n, e), qual è la lunghezza massima di un messaggio che possiamo cifrare con tale chiave? Dobbiamo assicurarci che la traduzione del messaggio in numero naturale x sia minore di n. La strategia è di confrontare le scritture di x e n in base 30.

Lunghezza dei messaggi cifrabili

Fissata una chiave pubblica (n, e), qual è la lunghezza massima di un messaggio che possiamo cifrare con tale chiave? Dobbiamo assicurarci che la traduzione del messaggio in numero naturale x sia minore di n. La strategia è di confrontare le scritture di x e n in base 30.

- Il numero di caratteri del messaggio corrisponde al numero di cifre di x in base 30.

Lunghezza dei messaggi cifrabili

Fissata una chiave pubblica (n, e), qual è la lunghezza massima di un messaggio che possiamo cifrare con tale chiave? Dobbiamo assicurarci che la traduzione del messaggio in numero naturale x sia minore di n. La strategia è di confrontare le scritture di x e n in base 30.

- Il numero di caratteri del messaggio corrisponde al numero di cifre di x in base 30.
- Il numero di cifre in base 30 di x è $\log_{30} x$. Il numero di cifre di n in base 30 è $\log_{30} n$.

Lunghezza dei messaggi cifrabili

Fissata una chiave pubblica (n, e), qual è la lunghezza massima di un messaggio che possiamo cifrare con tale chiave? Dobbiamo assicurarci che la traduzione del messaggio in numero naturale x sia minore di n. La strategia è di confrontare le scritture di x e n in base 30.

- Il numero di caratteri del messaggio corrisponde al numero di cifre di x in base 30.
- Il numero di cifre in base 30 di x è $\log_{30} x$. Il numero di cifre di n in base 30 è $\log_{30} n$.
- Quindi se $\log_{30} x < \log_{30} n$, sicuramente $x < n$.

Lunghezza dei messaggi cifrabili

Fissata una chiave pubblica (n, e), qual è la lunghezza massima di un messaggio che possiamo cifrare con tale chiave? Dobbiamo assicurarci che la traduzione del messaggio in numero naturale x sia minore di n. La strategia è di confrontare le scritture di x e n in base 30.

- Il numero di caratteri del messaggio corrisponde al numero di cifre di x in base 30.
- Il numero di cifre in base 30 di x è $\log_{30} x$. Il numero di cifre di n in base 30 è $\log_{30} n$.
- Quindi se $\log_{30} x < \log_{30} n$, sicuramente $x < n$.

Concludendo, *con la chiave pubblica (n, e), possiamo cifrare messaggi con al più $\log_{30} n$ caratteri.*