Introduzione alla Crittografia

Progetto Lauree Scientifiche

Liceo Scientifico "N. Tron", 23 gennaio 2007

Introduzione

Problema: A deve fare arrivare a B un certo messaggio, senza che C venga a conoscenza del contenuto.

Introduzione

Problema: A deve fare arrivare a B un certo messaggio, senza che C venga a conoscenza del contenuto.

Soluzione: A codifica il messaggio in base a regole concordate tra A e B e spedisce il messaggio a B.

Introduzione

Problema: A deve fare arrivare a B un certo messaggio, senza che C venga a conoscenza del contenuto.

Soluzione: A codifica il messaggio in base a regole concordate tra A e B e spedisce il messaggio a B. B, conoscendo le regole di cifratura , è in grado di decodificare il messaggio e risalire all'originale.

Introduzione

Problema: A deve fare arrivare a B un certo messaggio, senza che C venga a conoscenza del contenuto.

Soluzione: A codifica il messaggio in base a regole concordate tra A e B e spedisce il messaggio a B. B, conoscendo le regole di cifratura , è in grado di decodificare il messaggio e risalire all'originale. Se C viene in possesso del messaggio cifrato ma non conosce le regole di cifratura, non è in grado di risalire al messaggio originale.

Terminologia

$$\mathcal{P} = \{\text{messaggi in forma originale}\}$$

$$\mathcal{C} = \{\text{messaggi in forma codificata}\}$$

Terminologia

$$\mathcal{P} = \{\text{messaggi in forma originale}\}$$

$$\mathcal{C} = \{\text{messaggi in forma codificata}\}$$

Sia f una funzione invertibile da $\mathcal{P}$ a $\mathcal{C}$

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

Terminologia

$$\mathcal{P} = \{\text{messaggi in forma originale}\}$$

$$\mathcal{C} = \{\text{messaggi in forma codificata}\}$$

Sia f una funzione invertibile da $\mathcal{P}$ a $\mathcal{C}$

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

La quaterna $(\mathcal{P}, \mathcal{C}, f, f^{-1})$ è detta crittosistema, la funzione f chiave di cifratura e la funzione f^{-1} chiave di decifrazione.

Metodo di Cesare

Esempi

Metodo di Cesare: Consideriamo l'alfabeto con 21 lettere. Sia $n \leq 21$ un intero fissato; data una lettera x, sia

$$f(x) = \begin{cases} x + n & \text{se } x + n \leq 21 \\ x + n - 21 & \text{se } x + n > 21 \end{cases}$$

Esempi

Metodo di Cesare: Consideriamo l'alfabeto con 21 lettere. Sia $n \leq 21$ un intero fissato; data una lettera x, sia

$$f(x) = \begin{cases} x + n & \text{se } x + n \leq 21 \\ x + n - 21 & \text{se } x + n > 21 \end{cases}$$

Chiavi possibili: 21.

Esempi

Metodo di Cesare: Consideriamo l'alfabeto con 21 lettere. Sia $n \leq 21$ un intero fissato; data una lettera x, sia

$$f(x) = \begin{cases} x + n & \text{se } x + n \leq 21 \\ x + n - 21 & \text{se } x + n > 21 \end{cases}$$

Chiavi possibili: 21.

Esempio: $n = 7$

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

Esempi

Metodo di Cesare: Consideriamo l'alfabeto con 21 lettere. Sia $n \leq 21$ un intero fissato; data una lettera x, sia

$$f(x) = \begin{cases} x + n & \text{se } x + n \leq 21 \\ x + n - 21 & \text{se } x + n > 21 \end{cases}$$

Chiavi possibili: 21.

Esempio: $n = 7$

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

GIULIO CESARE $\longrightarrow$ PRESRV LNCHBN

Esempi

Esempi

Cifratura Monoalfabetica

Esempi

Cifratura Monoalfabetica: Consideriamo un qualsiasi riordinamento dell'alfabeto fissato, e si sostituisca ogni lettera con la lettera corrispondente.

Esempi

Cifratura Monoalfabetica: Consideriamo un qualsiasi riordinamento dell'alfabeto fissato, e si sostituisca ogni lettera con la lettera corrispondente.

Chiavi possibili: 21!

Esempi

Cifratura Monoalfabetica: Consideriamo un qualsiasi riordinamento dell'alfabeto fissato, e si sostituisca ogni lettera con la lettera corrispondente.

Chiavi possibili: 21!

Esempio:

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

Esempi

Cifratura Monoalfabetica: Consideriamo un qualsiasi riordinamento dell'alfabeto fissato, e si sostituisca ogni lettera con la lettera corrispondente.

Chiavi possibili: 21!

Esempio:

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

CIAO $\longrightarrow$ RAQG

Metodo di Vigenère

Esempi

Metodo di Vigenère: Fissiamo una qualsiasi parola come chiave di cifratura, ad esempio SOLE.

Esempi

Metodo di Vigenère: Fissiamo una qualsiasi parola come chiave di cifratura, ad esempio SOLE.

Questa parola individua 4 funzioni del tipo "Cesare": $f_1 = x + 17$, $f_2 = x + 13$, $f_3 = x + 10$, $f_4 = x + 5$.

Esempi

Metodo di Vigenère: Fissiamo una qualsiasi parola come chiave di cifratura, ad esempio SOLE.

Questa parola individua 4 funzioni del tipo "Cesare": $f_1 = x + 17$, $f_2 = x + 13$, $f_3 = x + 10$, $f_4 = x + 5$.

Per cifrare un messaggio con questa chiave, la prima lettera si cifra con f_1, la seconda con f_2, la terza con f_3, la quarta con f_4, la quinta con f_1, la sesta con f_2, ...

Esempi

Metodo di Vigenère: Fissiamo una qualsiasi parola come chiave di cifratura, ad esempio SOLE.

Questa parola individua 4 funzioni del tipo "Cesare": $f_1 = x + 17$, $f_2 = x + 13$, $f_3 = x + 10$, $f_4 = x + 5$.

Per cifrare un messaggio con questa chiave, la prima lettera si cifra con f_1, la seconda con f_2, la terza con f_3, la quarta con f_4, la quinta con f_1, la sesta con f_2, ...

Esempio: QUESTO METODO NON È SICURO $\longrightarrow$ MMQA PEZB ....

Esempi

Metodo di Vigenère: Fissiamo una qualsiasi parola come chiave di cifratura, ad esempio SOLE.

Questa parola individua 4 funzioni del tipo "Cesare": $f_1 = x + 17$, $f_2 = x + 13$, $f_3 = x + 10$, $f_4 = x + 5$.

Per cifrare un messaggio con questa chiave, la prima lettera si cifra con f_1, la seconda con f_2, la terza con f_3, la quarta con f_4, la quinta con f_1, la sesta con f_2, ...

Esempio: QUESTO METODO NON È SICURO $\longrightarrow$ MMQA PEZB ....

Possibili chiavi: infinite.

Problemi

Problemi

1. La cifratura di Cesare è facilmente decifrabile, dato il numero ristretto di possibili chiavi

Problemi

1. La cifratura di Cesare è facilmente decifrabile, dato il numero ristretto di possibili chiavi
2. Le cifrature monoalfabetiche e di Vigenère, pur avendo un numero elevato di possibili chiavi, sono decifrabili tramite considerazioni di tipo linguistico (ripetizioni di gruppi di lettere, analisi delle frequenze, . . .)

Problemi

1. La cifratura di Cesare è facilmente decifrabile, dato il numero ristretto di possibili chiavi
2. Le cifrature monoalfabetiche e di Vigenère, pur avendo un numero elevato di possibili chiavi, sono decifrabili tramite considerazioni di tipo linguistico (ripetizioni di gruppi di lettere, analisi delle frequenze, . . .)
3. Anche complicando notevolmente i precedenti sistemi di cifratura, la conoscenza del messaggio cifrato e della chiave di cifratura comporta la decifrazione del messaggio. Pertanto la chiave di cifratura deve rimanere segreta

Problemi

1. La cifratura di Cesare è facilmente decifrabile, dato il numero ristretto di possibili chiavi
2. Le cifrature monoalfabetiche e di Vigenère, pur avendo un numero elevato di possibili chiavi, sono decifrabili tramite considerazioni di tipo linguistico (ripetizioni di gruppi di lettere, analisi delle frequenze, . . .)
3. Anche complicando notevolmente i precedenti sistemi di cifratura, la conoscenza del messaggio cifrato e della chiave di cifratura comporta la decifrazione del messaggio. Pertanto la chiave di cifratura deve rimanere segreta

Il problema maggiore è quello della distribuzione delle chiavi

Da chiave privata a chiave pubblica

Come rendere sicuro lo scambio delle chiavi?

Da chiave privata a chiave pubblica

Come rendere sicuro lo scambio delle chiavi?

1. A spedisce il messaggio a B all'interno di una scatola chiusa con un lucchetto L_A, di cui solo A possiede la chiave

Da chiave privata a chiave pubblica

Come rendere sicuro lo scambio delle chiavi?

1. A spedisce il messaggio a B all'interno di una scatola chiusa con un lucchetto L_A, di cui solo A possiede la chiave
2. B riceve la scatola chiusa con L_A, aggiunge un altro lucchetto L_B, di cui solo B ha la chiave, e rispedisce la scatola a A

Da chiave privata a chiave pubblica

Come rendere sicuro lo scambio delle chiavi?

1. A spedisce il messaggio a B all'interno di una scatola chiusa con un lucchetto L_A, di cui solo A possiede la chiave
2. B riceve la scatola chiusa con L_A, aggiunge un altro lucchetto L_B, di cui solo B ha la chiave, e rispedisce la scatola a A
3. A, ricevuta la scatola con il doppio lucchetto, toglie L_A e rispedisce la scatola a B

Da chiave privata a chiave pubblica

Come rendere sicuro lo scambio delle chiavi?

1. A spedisce il messaggio a B all'interno di una scatola chiusa con un lucchetto L_A, di cui solo A possiede la chiave
2. B riceve la scatola chiusa con L_A, aggiunge un altro lucchetto L_B, di cui solo B ha la chiave, e rispedisce la scatola a A
3. A, ricevuta la scatola con il doppio lucchetto, toglie L_A e rispedisce la scatola a B
4. B toglie il lucchetto L_B, apre la scatola e legge il messaggio

Da chiave privata a chiave pubblica

Come eliminare lo scambio delle chiavi?

Da chiave privata a chiave pubblica

Come eliminare lo scambio delle chiavi?

1. A spedisce a tutte le persone con cui desidera comunicare una copia di un lucchetto L_A, di cui solo A possiede la chiave

Da chiave privata a chiave pubblica

Come eliminare lo scambio delle chiavi?

1. A spedisce a tutte le persone con cui desidera comunicare una copia di un lucchetto L_A, di cui solo A possiede la chiave
2. Se B vuole spedire un messaggio ad A, lo mette in una scatola e la chiude con L_A.

Da chiave privata a chiave pubblica

Come eliminare lo scambio delle chiavi?

1. A spedisce a tutte le persone con cui desidera comunicare una copia di un lucchetto L_A, di cui solo A possiede la chiave
2. Se B vuole spedire un messaggio ad A, lo mette in una scatola e la chiude con L_A.
3. A, ricevuta la scatola, toglie L_A con la chiave che solo lui possiede, apre la scatola e legge il messaggio.

RSA (Rivest, Shamir e Adleman)

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

1. A costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica la chiave di cifratura f

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

1. A costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica la chiave di cifratura f
2. Se B vuole comunicare con A, codifica il messaggio usando f e lo spedisce a A

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

1. A costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica la chiave di cifratura f
2. Se B vuole comunicare con A, codifica il messaggio usando f e lo spedisce a A
3. A decodifica il messaggio usando la chiave di decifrazione f^{-1}, nota solo a lui

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

1. A costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica la chiave di cifratura f
2. Se B vuole comunicare con A, codifica il messaggio usando f e lo spedisce a A
3. A decodifica il messaggio usando la chiave di decifrazione f^{-1}, nota solo a lui
4. Sistema a chiave pubblica

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

1. A costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica la chiave di cifratura f
2. Se B vuole comunicare con A, codifica il messaggio usando f e lo spedisce a A
3. A decodifica il messaggio usando la chiave di decifrazione f^{-1}, nota solo a lui
4. Sistema a chiave pubblica
   - f è detta chiave pubblica

RSA (Rivest, Shamir e Adleman)

Il sistema si basa sull'esistenza di funzioni f per cui è molto complicato determinare f^{-1}, conoscendo solo f

1. A costruisce una coppia (f, f^{-1}) che soddisfa la precedente proprietà, e rende pubblica la chiave di cifratura f
2. Se B vuole comunicare con A, codifica il messaggio usando f e lo spedisce a A
3. A decodifica il messaggio usando la chiave di decifrazione f^{-1}, nota solo a lui
4. Sistema a chiave pubblica
   - f è detta chiave pubblica
   - f^{-1} è detta chiave privata

Schema delle lezioni

Schema delle lezioni

- Lezione 1: Metodi crittografici classici a chiave privata. Aritmetica modulare.

Schema delle lezioni

- Lezione 1: Metodi crittografici classici a chiave privata. Aritmetica modulare.
- Lezione 2: Algoritmo di Euclide, Piccolo Teorema di Fermat, fattorizzazione in fattori primi

Schema delle lezioni

- Lezione 1: Metodi crittografici classici a chiave privata. Aritmetica modulare.
- Lezione 2: Algoritmo di Euclide, Piccolo Teorema di Fermat, fattorizzazione in fattori primi
- Lezione 3: Sistemi a chiave pubblica; RSA

Schema delle lezioni

- Lezione 1: Metodi crittografici classici a chiave privata. Aritmetica modulare.
- Lezione 2: Algoritmo di Euclide, Piccolo Teorema di Fermat, fattorizzazione in fattori primi
- Lezione 3: Sistemi a chiave pubblica; RSA
- Lezione 4: Firma digitale