Introduzione alla crittografia

Gianfranco Gallizia

6 Giugno 2024

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Non sono un avvocato nè un crittoanalista. Tutto quello che troverete scritto in queste slide e sentirete durante la presentazione è frutto di un'opera di ricerca che, per quanto accurata, non ha la pretesa di essere corretta in ogni sua singola parte.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Non sono un avvocato nè un crittoanalista. Tutto quello che troverete scritto in queste slide e sentirete durante la presentazione è frutto di un'opera di ricerca che, per quanto accurata, non ha la pretesa di essere corretta in ogni sua singola parte.

In caso di dubbi consultate un professionista.

Presentazioni

Ma chi sei tu?

Presentazioni

Ma chi sei tu?

Chi sono:

Presentazioni

Ma chi sei tu?

Chi sono:

- Tecnico informatico

Presentazioni

Ma chi sei tu?

Chi sono:

- Tecnico informatico
- Sviluppatore (sono avezzo a C, C++ e so un po' di C#)

Presentazioni

Ma chi sei tu?

Chi sono:

- Tecnico informatico
- Sviluppatore (sono avezzo a C, C++ e so un po' di C#)
- Sistemista *NIX (Debian GNU/Linux, Alma/CentOS e nel tempo libero FreeBSD e OpenBSD)

Presentazioni

Ma chi sei tu?

Chi sono:

- Tecnico informatico
- Sviluppatore (sono avezzo a C, C++ e so un po' di C#)
- Sistemista *NIX (Debian GNU/Linux, Alma/CentOS e nel tempo libero FreeBSD e OpenBSD)
- Scripter in bash, Tcl/Tk e Python alla bisogna

Presentazioni

Ma chi sei tu?

Chi sono:

- Tecnico informatico
- Sviluppatore (sono avezzo a C, C++ e so un po' di C#)
- Sistemista *NIX (Debian GNU/Linux, Alma/CentOS e nel tempo libero FreeBSD e OpenBSD)
- Scripter in bash, Tcl/Tk e Python alla bisogna
- Molto tempo fa ho scritto orrori in PHP e Django ma devo ancora provare l'ebbrezza di Node.js (il web development non è il mio forte)

Introduzione

Di cosa ci parlerai?

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione

Di cosa ci parlerai?

Di cosa parlerò:

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa parlerò:

- Un po' di storia

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa parlerò:

- Un po' di storia
- Crittografia a chiave simmetrica

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa parlerò:

- Un po' di storia
- Crittografia a chiave simmetrica
- Crittografia a chiave asimmetrica

Introduzione

Di cosa ci parlerai?

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa parlerò:

- Un po' di storia
- Crittografia a chiave simmetrica
- Crittografia a chiave asimmetrica
- Hash e firma crittografica

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa parlerò:

- Un po' di storia
- Crittografia a chiave simmetrica
- Crittografia a chiave asimmetrica
- Hash e firma crittografica
- Conclusioni

Introduzione

Di cosa NON ci parlerai?

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

- Quanti e quali tools di crittografia esistono

Introduzione

Di cosa NON ci parlerai?

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

- Quanti e quali tools di crittografia esistono
- Come si usano i tools suddetti

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

- Quanti e quali tools di crittografia esistono
- Come si usano i tools suddetti
- Come si fa a recuperare un messaggio criptato senza avere la chiave

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

- Quanti e quali tools di crittografia esistono
- Come si usano i tools suddetti
- Come si fa a recuperare un messaggio criptato senza avere la chiave
- Come si fa ad usare la firma digitale

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

- Quanti e quali tools di crittografia esistono
- Come si usano i tools suddetti
- Come si fa a recuperare un messaggio criptato senza avere la chiave
- Come si fa ad usare la firma digitale
- Come si fa ad ottenere un certificato TLS valido per www.google.com

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Di cosa NON parlerò:

- Quanti e quali tools di crittografia esistono
- Come si usano i tools suddetti
- Come si fa a recuperare un messaggio criptato senza avere la chiave
- Come si fa ad usare la firma digitale
- Come si fa ad ottenere un certificato TLS valido per www.google.com
- Come si fa a fare soldi con Bitcoin

Un po' di storia

Gli albori

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problema

Un po' di storia

Gli albori

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problema

Come faccio a fare in modo che un mio messaggio arrivi a chi di dovere senza che nessun altro ne venga a conoscenza?

Un po' di storia

Gli albori

Problema

Come faccio a fare in modo che un mio messaggio arrivi a chi di dovere senza che nessun altro ne venga a conoscenza?

Soluzione

Un po' di storia

Gli albori

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problema

Come faccio a fare in modo che un mio messaggio arrivi a chi di dovere senza che nessun altro ne venga a conoscenza?

Soluzione

Scrivo il messaggio in modo che sia illeggibile a chiunque altro concordando con il destinatario un metodo per criptare (nascondere) e decriptare (rivelare) il messaggio stesso.

Un po' di storia

Antichità

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il codice atbash

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il codice atbash

Da Wikipedia (`https://it.wikipedia.org/wiki/Atbash`):

> *L'atbash è un semplice cifrario a sostituzione monoalfabetica in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.*

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il codice atbash

Da Wikipedia (`https://it.wikipedia.org/wiki/Atbash`):

> *L'atbash è un semplice cifrario a sostituzione monoalfabetica in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.*

In pratica si passa da:

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

a:

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

Un po' di storia

Antichità

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il codice atbash

Da Wikipedia (`https://it.wikipedia.org/wiki/Atbash`):

> *L'atbash è un semplice cifrario a sostituzione monoalfabetica in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.*

In pratica si passa da:
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
a:
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Esempio

GIRVHGV = TRIESTE

Un po' di storia

Antichità

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il cifrario di Cesare

Un po' di storia

Antichità

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il cifrario di Cesare

Il cifrario a rotazione o cifrario di Cesare (perché utilizzato da quest'ultimo durante la conquista della Gallia) è un cifrario monoalfabetico a sostituzione in cui le lettere vengono spostate di un numero prestabilito di posizioni in avanti in fase di criptazione e dello stesso numero di posizioni in indietro in fase di decriptazione.

Un po' di storia

Antichità

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

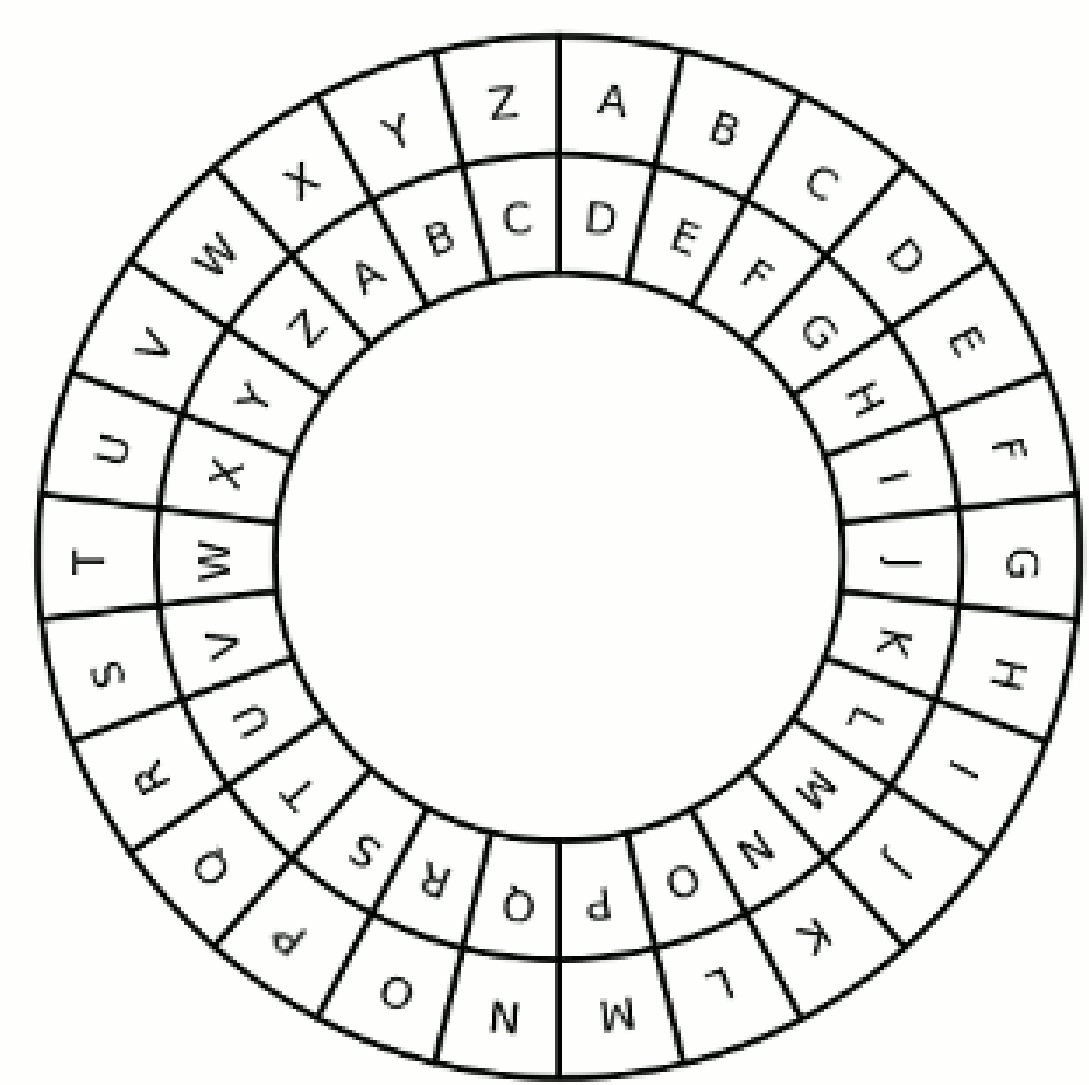
Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni



Un po' di storia

Antichità

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problemi dei cifrari monoalfabetici a sostituzione

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi dei cifrari monoalfabetici a sostituzione

Sia il cifrario atbash che il cifrario di Cesare soffrono dello stesso problema: sono deboli ad attacchi statistici. Se si conosce il linguaggio utilizzato per scrivere il messaggio (e questo è abbastanza lungo) si possono ricavare le frequenze approssimate delle lettere ed inferire il testo del messaggio in chiaro in virtù del principio che lettere uguali sono codificate nello stesso modo.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi dei cifrari monoalfabetici a sostituzione

Sia il cifrario atbash che il cifrario di Cesare soffrono dello stesso problema: sono deboli ad attacchi statistici. Se si conosce il linguaggio utilizzato per scrivere il messaggio (e questo è abbastanza lungo) si possono ricavare le frequenze approssimate delle lettere ed inferire il testo del messaggio in chiaro in virtù del principio che lettere uguali sono codificate nello stesso modo.

Al giorno d'oggi questi cifrari sono per lo più appannaggio di riviste di enigmistica ed affini.

Crittografia a chiave simmetrica

Digressione: l'OR esclusivo

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

XOR

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

Proprietà:

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Proprietà:

- $A \oplus B = B \oplus A$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Proprietà:

- $A \oplus B = B \oplus A$
- $A \oplus 0 = A$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Proprietà:

- $A \oplus B = B \oplus A$
- $A \oplus 0 = A$
- $A \oplus 1 = \neg A$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

XOR

L'operazione logica di OR esclusivo (XOR o $\oplus$) è sintetizzabile con la frase: *"Se gli argomenti sono diversi allora il risultato è vero, altrimenti no"*.

A	B	X
0	0	0
1	0	1
0	1	1
1	1	0

Proprietà:

- $A \oplus B = B \oplus A$
- $A \oplus 0 = A$
- $A \oplus 1 = \neg A$
- $A \oplus B = X \rightarrow X \oplus B = A$

Crittografia a chiave simmetrica

Digressione: l'OR esclusivo

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Definiamo:

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Definiamo:

- M *messaggio*

Crittografia a chiave simmetrica

Digressione: l'OR esclusivo

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Definiamo:

- M *messaggio*
- K *chiave*

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Definiamo:

- M *messaggio*
- K *chiave*
- C *testo cifrato*

Crittografia a chiave simmetrica

Digressione: l'OR esclusivo

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Definiamo:

- M *messaggio*
- K *chiave*
- C *testo cifrato*

E applichiamo questa proprietà ad ogni bit di M, K e C:

$m \oplus k = c \rightarrow c \oplus k = m$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Definiamo:

- M *messaggio*
- K *chiave*
- C *testo cifrato*

E applichiamo questa proprietà ad ogni bit di M, K e C:
$m \oplus k = c \rightarrow c \oplus k = m$

K ci consente di passare da M a C e viceversa.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Definiamo:

- M *messaggio*
- K *chiave*
- C *testo cifrato*

E applichiamo questa proprietà ad ogni bit di M, K e C:

$m \oplus k = c \rightarrow c \oplus k = m$

K ci consente di passare da M a C e viceversa.

(Purché K abbia la stessa lunghezza di M)

Crittografia a chiave simmetrica

One Time Pad

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

One Time Pad

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

One Time Pad

Se usiamo una chiave K diversa per ogni singolo messaggio M abbiamo un One Time Pad.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

One Time Pad

Se usiamo una chiave K diversa per ogni singolo messaggio M abbiamo un One Time Pad.
Questo tipo di cifrario è un *cifrario perfetto*, ossia matematichese per dire che l'unica maniera per decifrare C ed ottenere M è conoscere K (esiste una dimostrazione formale di questo).

Crittografia a chiave simmetrica

One Time Pad - Problemi

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi

- K lunga quanto M significa che se devo criptare 4 Terabyte di dati ho bisogno di una chiave lunga altrettanto.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi

- K lunga quanto M significa che se devo criptare 4 Terabyte di dati ho bisogno di una chiave lunga altrettanto.
- Non posso riutilizzare le chiavi pena una drastica riduzione della complessità di decriptazione per un terzo malintenzionato.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi

- K lunga quanto M significa che se devo criptare 4 Terabyte di dati ho bisogno di una chiave lunga altrettanto.
- Non posso riutilizzare le chiavi pena una drastica riduzione della complessità di decriptazione per un terzo malintenzionato.
- Come trasmetto 4 Terabyte di chiave in maniera sicura al mio interlocutore fidato?

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problemi

- K lunga quanto M significa che se devo criptare 4 Terabyte di dati ho bisogno di una chiave lunga altrettanto.
- Non posso riutilizzare le chiavi pena una drastica riduzione della complessità di decriptazione per un terzo malintenzionato.
- Come trasmetto 4 Terabyte di chiave in maniera sicura al mio interlocutore fidato?
- Messaggi brevi significa chiavi brevi. Chiavi brevi sono più facili da scoprire (devo generare un numero inferiore di combinazioni).

Crittografia a chiave simmetrica

One Time Pad - Lezioni apprese

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Lezioni apprese

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Lezioni apprese

- Privilegiare chiavi "lunghe".

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Lezioni apprese

- Privilegiare chiavi "lunghe".
- Una buona chiave è una chiave difficile da derivare.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Lezioni apprese

- Privilegiare chiavi "lunghe".
- Una buona chiave è una chiave difficile da derivare.
- Un buon generatore di numeri casuali genera buone chiavi.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Lezioni apprese

- Privilegiare chiavi "lunghe".
- Una buona chiave è una chiave difficile da derivare.
- Un buon generatore di numeri casuali genera buone chiavi.
- Se la chiave è più breve del testo dobbiamo escogitare un modo per utilizzarla.

Crittografia a chiave simmetrica

Cifrari simmetrici

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Cifrari simmetrici (in ordine cronologico)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Cifrari simmetrici (in ordine cronologico)

- 1975 - DES. (Insicuro)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Cifrari simmetrici (in ordine cronologico)

- 1975 - DES. (Insicuro)
- 1978 - 3-DES. (Insicuro)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Cifrari simmetrici (in ordine cronologico)

- 1975 - DES. (Insicuro)
- 1978 - 3-DES. (Insicuro)
- 1993 - Blowfish. (Libero da brevetti e di pubblico dominio)

Crittografia a chiave simmetrica

Cifrari simmetrici

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Cifrari simmetrici (in ordine cronologico)

- 1975 - DES. (Insicuro)
- 1978 - 3-DES. (Insicuro)
- 1993 - Blowfish. (Libero da brevetti e di pubblico dominio)
- 1998 - AES. (Standard attualmente in uso)

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Data Encryption Standard

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Data Encryption Standard

- Ideato nei primi anni 70 da IBM su un'idea di Horst Feistel.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Data Encryption Standard

- Ideato nei primi anni 70 da IBM su un'idea di Horst Feistel.
- Il DES è un cifrario a blocchi: il testo in chiaro viene spezzato in blocchi da 64 bit e criptato un blocco alla volta.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Data Encryption Standard

- Ideato nei primi anni 70 da IBM su un'idea di Horst Feistel.
- Il DES è un cifrario a blocchi: il testo in chiaro viene spezzato in blocchi da 64 bit e criptato un blocco alla volta.
- A seguito dell'intervento della NSA la lunghezza della chiave fu portata da 128 bit a 56 bit più 8 bit di parità (portando il totale a 64 bit).

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Data Encryption Standard

- Ideato nei primi anni 70 da IBM su un'idea di Horst Feistel.
- Il DES è un cifrario a blocchi: il testo in chiaro viene spezzato in blocchi da 64 bit e criptato un blocco alla volta.
- A seguito dell'intervento della NSA la lunghezza della chiave fu portata da 128 bit a 56 bit più 8 bit di parità (portando il totale a 64 bit).
- Il DES è il primo cifrario a rete di Feistel e la sua struttura sarà replicata nel triplo DES (3-DES) e in Blowfish.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

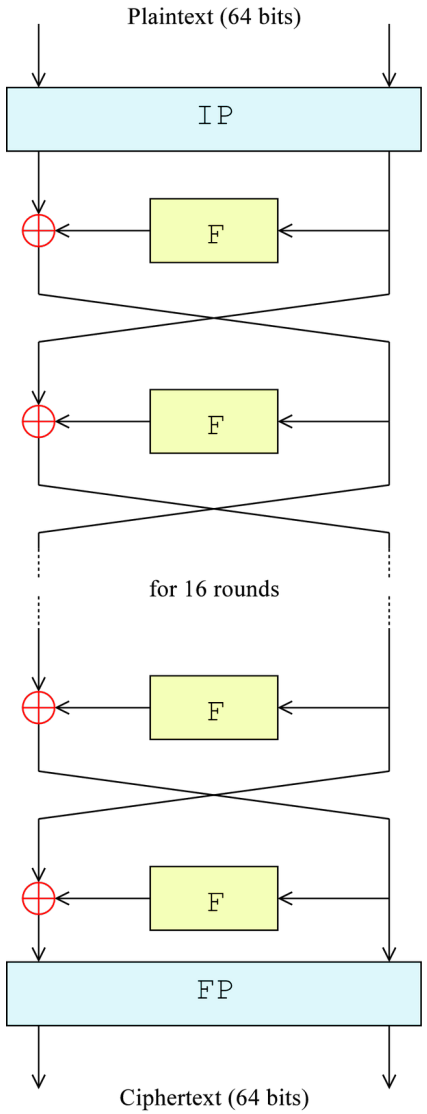
Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

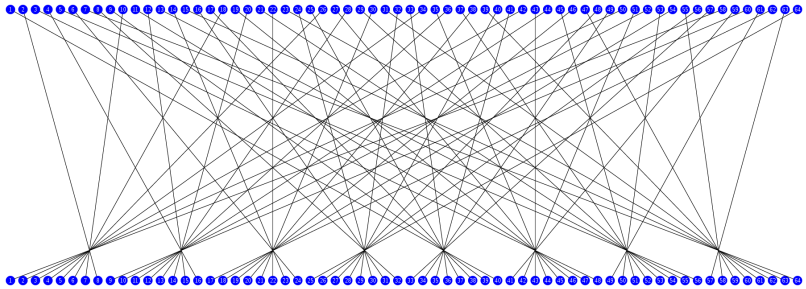
Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

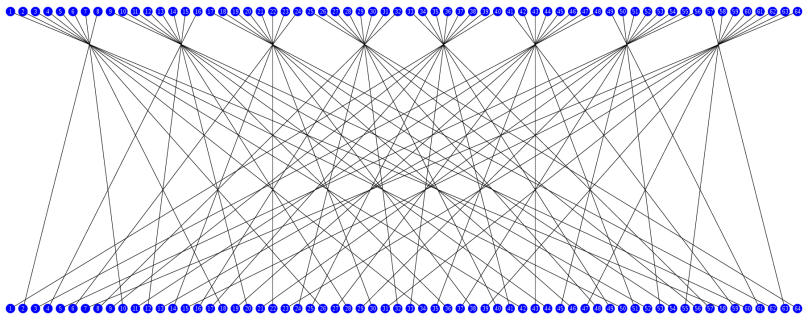


Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

IP (Initial Permutation)

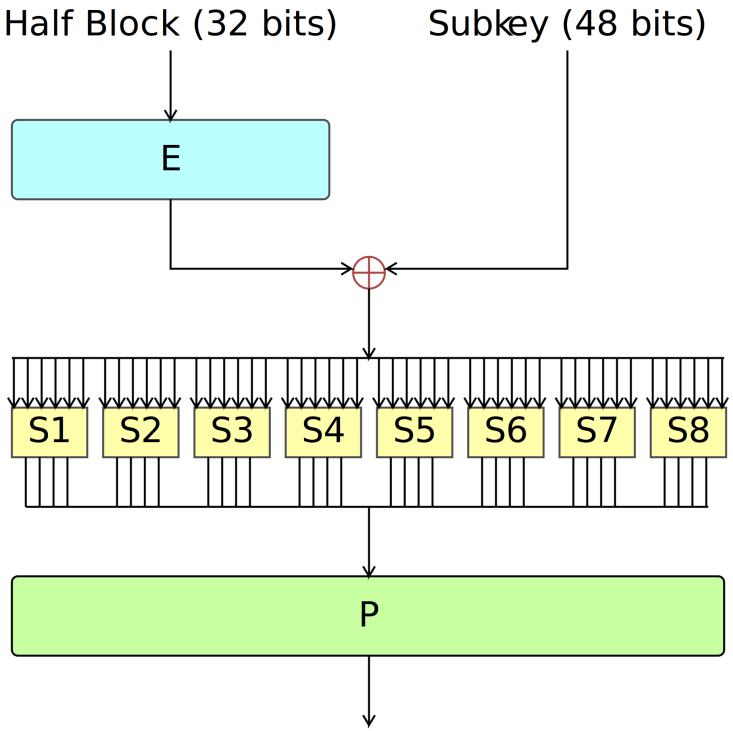


FP (Final Permutation)



Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

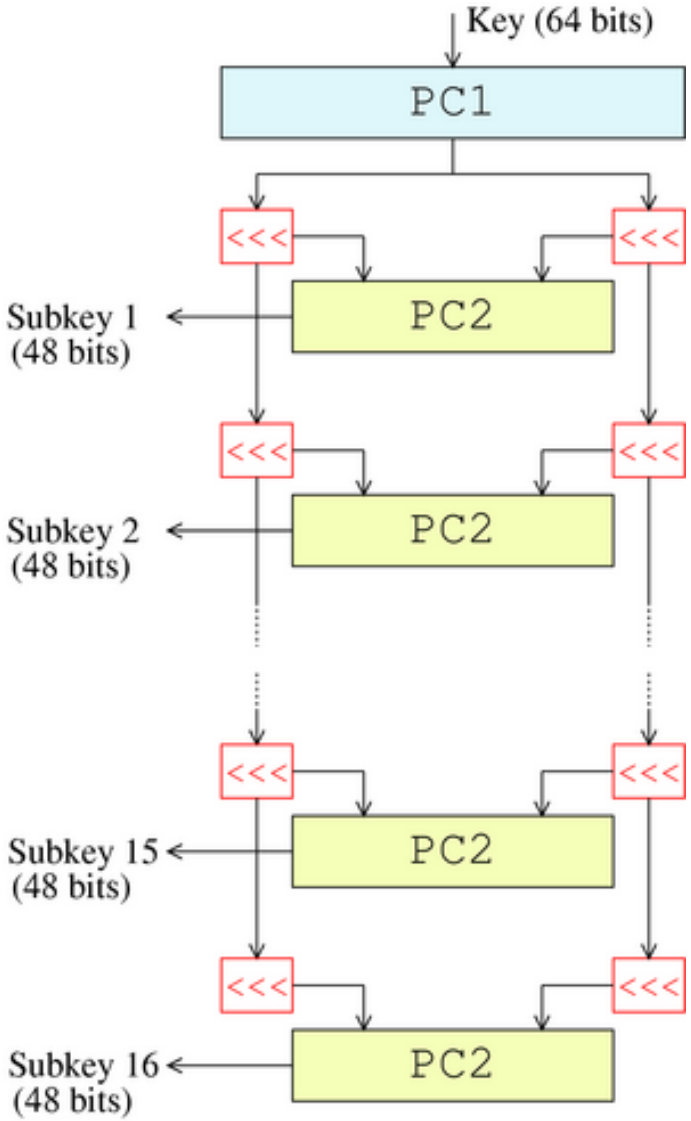
Funzione di Feistel



Crittografia a chiave simmetrica

Cifrari simmetrici - DES

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni



Crittografia a chiave simmetrica

Cifrari simmetrici - AES

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

AES

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

AES

- Cifrario a blocco nato per sostituire DES

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

AES

- Cifrario a blocco nato per sostituire DES
- I blocchi sono sempre lunghi 128 bit

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

AES

- Cifrario a blocco nato per sostituire DES
- I blocchi sono sempre lunghi 128 bit
- La chiave può essere lunga 128, 192 o 256 bit

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

AES

- Cifrario a blocco nato per sostituire DES
- I blocchi sono sempre lunghi 128 bit
- La chiave può essere lunga 128, 192 o 256 bit
- Ad oggi le migliori tecniche di attacco contro AES sono del tipo side-channel

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

AES

- Cifrario a blocco nato per sostituire DES
- I blocchi sono sempre lunghi 128 bit
- La chiave può essere lunga 128, 192 o 256 bit
- Ad oggi le migliori tecniche di attacco contro AES sono del tipo side-channel
- Tecniche matematiche che attaccano l'algoritmo riducono lo spazio di ricerca delle chiavi di 2 bit

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problema

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problema

Ho un testo da cifrare che è più lungo del blocco definito dallo standard che sto utilizzando.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Problema

Ho un testo da cifrare che è più lungo del blocco definito dallo standard che sto utilizzando.
Come faccio a cifrarlo tutto?

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problema

Ho un testo da cifrare che è più lungo del blocco definito dallo standard che sto utilizzando.
Come faccio a cifrarlo tutto?

Soluzione (banale)

Divido il testo in chiaro in blocchi e applico la cifratura ad ogni blocco usando sempre la stessa chiave.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

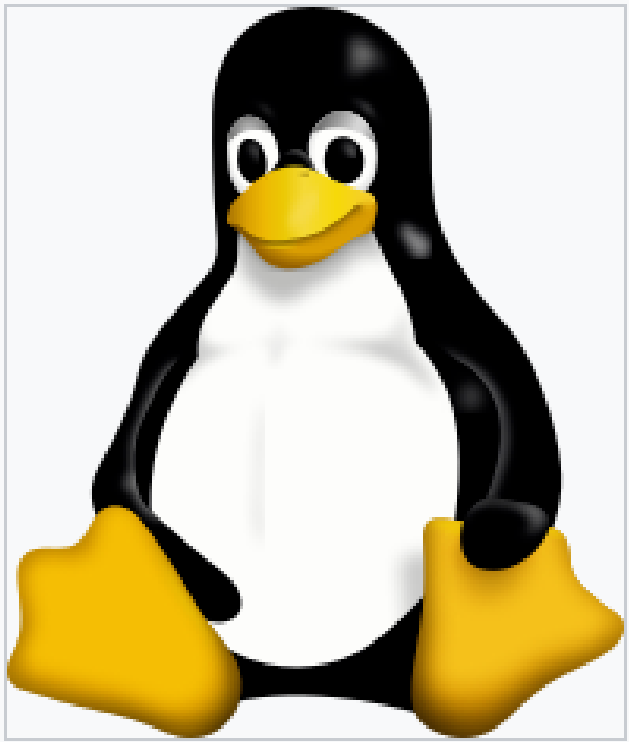
Un po' di storia

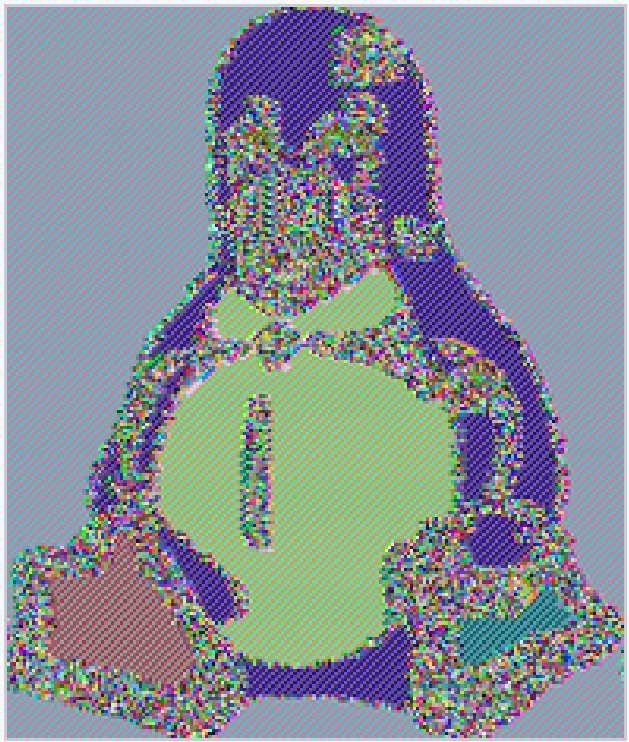
Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni





Crittografia a chiave simmetrica

Cifrari simmetrici - CBC

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Domanda

Possiamo riutilizzare la chiave senza riutilizzare la chiave?

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

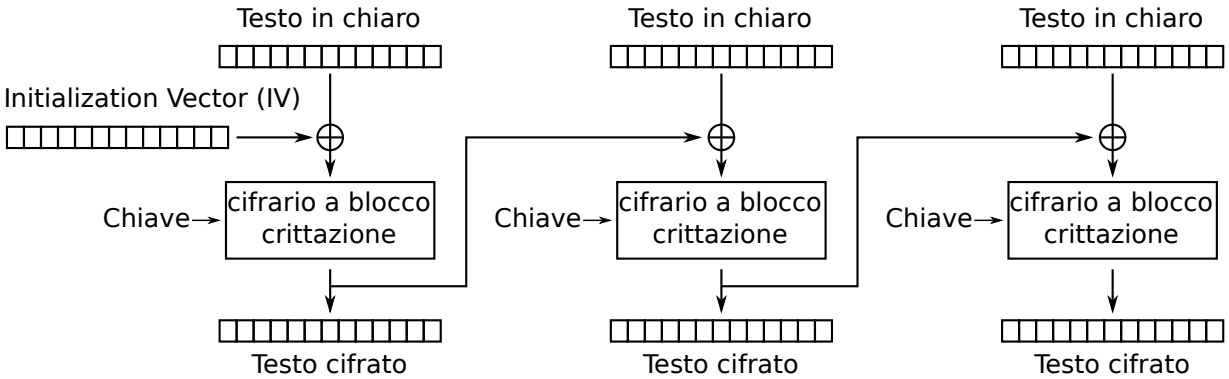
Domanda

Possiamo riutilizzare la chiave senza riutilizzare la chiave?

Risposta

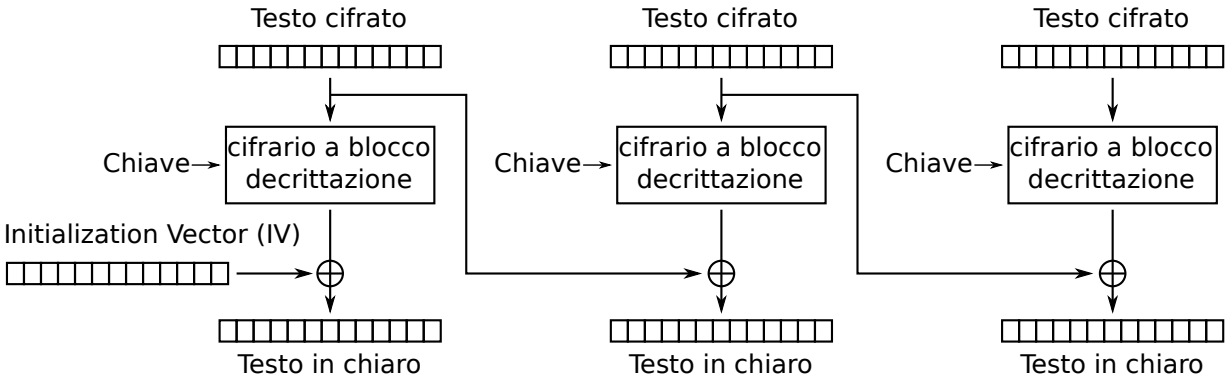
Sì, riutilizzando il blocco cifrato precedentemente come chiave per uno XOR.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni



Cipher Block Chaining (CBC) - Crittazione

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni



Cipher Block Chaining (CBC) - Decrittazione

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Problema

Non si può parallelizzare la crittazione usando il CBC.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

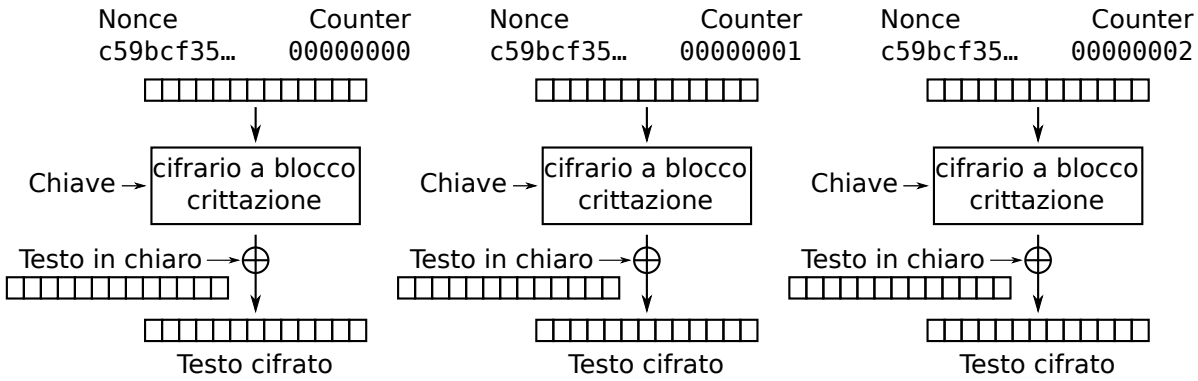
Problema

Non si può parallelizzare la crittazione usando il CBC.

Soluzione

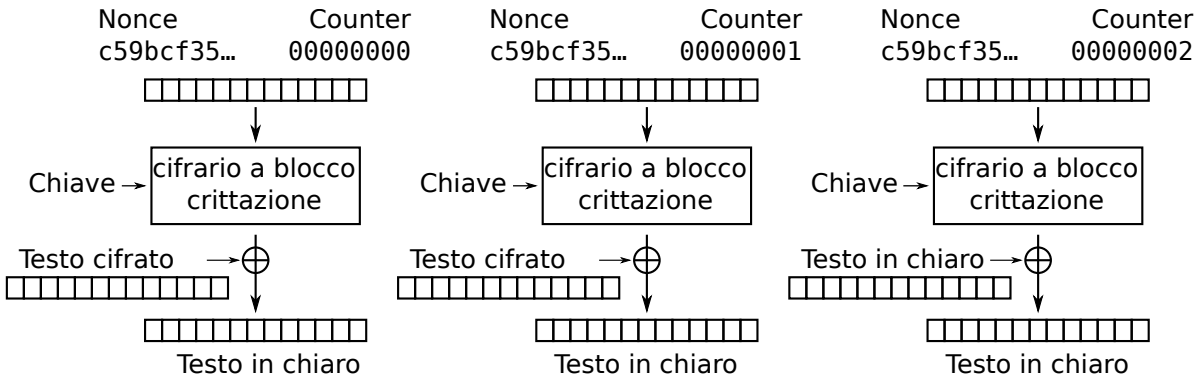
Usare uno schema di crittazione diverso: CTR.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni



Counter (CTR) - crittazione

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni



Counter (CTR) - decrittazione

Crittografia a chiave simmetrica

Il problema della chiave

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il problema della chiave

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il problema della chiave

Come faccio a trasferire in modo sicuro la chiave crittografica?

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il problema della chiave

Come faccio a trasferire in modo sicuro la chiave crittografica?

- Tramite un canale sicuro (come faccio a stabilire se è sicuro?)

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il problema della chiave

Come faccio a trasferire in modo sicuro la chiave crittografica?

- Tramite un canale sicuro (come faccio a stabilire se è sicuro?)
- Criptando la chiave (con che altra chiave?)

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Il problema della chiave

Come faccio a trasferire in modo sicuro la chiave crittografica?

- Tramite un canale sicuro (come faccio a stabilire se è sicuro?)
- Criptando la chiave (con che altra chiave?)
- In un altro modo (quale?)

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Divisione tra numeri naturali

$$D \div d = Q + r$$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Divisione tra numeri naturali

$$D \div d = Q + r$$

- D dividendo, d divisore, Q quoziente, r resto.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Divisione tra numeri naturali

$$D \div d = Q + r$$

- D dividendo, d divisore, Q quoziente, r resto.
- $r < d$ assicura che il risultato sia unico.

Crittografia a chiave simmetrica

Digressione: l'operazione modulo

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Divisione tra numeri naturali

$$D \div d = Q + r$$

- D dividendo, d divisore, Q quoziente, r resto.
- $r < d$ assicura che il risultato sia unico.

Modulo

$$D \bmod d = r$$

Crittografia a chiave simmetrica

Scambio Diffie-Hellman

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$
3. Alice invia a Bob A, g e p

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$
3. Alice invia a Bob A, g e p
4. Bob sceglie un numero segreto b

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$
3. Alice invia a Bob A, g e p
4. Bob sceglie un numero segreto b
5. Bob calcola $B = g^b \bmod p$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$
3. Alice invia a Bob A, g e p
4. Bob sceglie un numero segreto b
5. Bob calcola $B = g^b \bmod p$
6. Bob invia ad Alice B

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$
3. Alice invia a Bob A, g e p
4. Bob sceglie un numero segreto b
5. Bob calcola $B = g^b \bmod p$
6. Bob invia ad Alice B
7. Alice calcola $K_a = B^a \bmod p$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman

Prendiamo due soggetti che vogliono comunicare in modo sicuro tra loro: Alice e Bob.

1. Alice sceglie un numero primo p, un generatore g ed un numero segreto a
2. Alice calcola $A = g^a \bmod p$
3. Alice invia a Bob A, g e p
4. Bob sceglie un numero segreto b
5. Bob calcola $B = g^b \bmod p$
6. Bob invia ad Alice B
7. Alice calcola $K_a = B^a \bmod p$
8. Bob calcola $K_b = A^b \bmod p$

Crittografia a chiave simmetrica

Scambio Diffie-Hellman

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Soluzione: lo Scambio Diffie-Hellman (continua)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman (continua)

$$K_a = B^a \bmod p = (g^b \bmod p)^a \bmod p =$$
$$= (g^b)^a \bmod p = g^{ba} \bmod p = g^{ab} \bmod p$$
$$K_b = A^b \bmod p = (g^a \bmod p)^b \bmod p =$$
$$= (g^a)^b \bmod p = g^{ab} \bmod p$$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman (continua)

$$K_a = B^a \bmod p = (g^b \bmod p)^a \bmod p =$$
$$= (g^b)^a \bmod p = g^{ba} \bmod p = g^{ab} \bmod p$$
$$K_b = A^b \bmod p = (g^a \bmod p)^b \bmod p =$$
$$= (g^a)^b \bmod p = g^{ab} \bmod p$$

$$K_a = K_b$$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Soluzione: lo Scambio Diffie-Hellman (continua)

$$K_a = B^a \bmod p = (g^b \bmod p)^a \bmod p =$$
$$= (g^b)^a \bmod p = g^{ba} \bmod p = g^{ab} \bmod p$$
$$K_b = A^b \bmod p = (g^a \bmod p)^b \bmod p =$$
$$= (g^a)^b \bmod p = g^{ab} \bmod p$$

$$K_a = K_b$$

Abbiamo scambiato la chiave senza **MAI** trasmetterla in chiaro tra Alice e Bob.

Crittografia a chiave asimmetrica

Due chiavi

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Due chiavi

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Due chiavi

E se invece di avere una sola chiave ne avessi due?

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Due chiavi

E se invece di avere una sola chiave ne avessi due?

- Una chiave deve poter decrittare i messaggi dell'altra e viceversa ma non deve poter decrittare i messaggi che essa stessa ha criptato.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Due chiavi

E se invece di avere una sola chiave ne avessi due?

- Una chiave deve poter decrittare i messaggi dell'altra e viceversa ma non deve poter decrittare i messaggi che essa stessa ha criptato.
- Una chiave la terrei al sicuro mentre distribuirei l'altra.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Due chiavi

E se invece di avere una sola chiave ne avessi due?

- Una chiave deve poter decrittare i messaggi dell'altra e viceversa ma non deve poter decrittare i messaggi che essa stessa ha criptato.
- Una chiave la terrei al sicuro mentre distribuirei l'altra.
- Chiunque potrebbe mandarmi messaggi sapendo che solo io posso leggerli.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Due chiavi

E se invece di avere una sola chiave ne avessi due?

- Una chiave deve poter decrittare i messaggi dell'altra e viceversa ma non deve poter decrittare i messaggi che essa stessa ha criptato.
- Una chiave la terrei al sicuro mentre distribuirei l'altra.
- Chiunque potrebbe mandarmi messaggi sapendo che solo io posso leggerli.

Problema

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Due chiavi

E se invece di avere una sola chiave ne avessi due?

- Una chiave deve poter decrittare i messaggi dell'altra e viceversa ma non deve poter decrittare i messaggi che essa stessa ha criptato.
- Una chiave la terrei al sicuro mentre distribuirei l'altra.
- Chiunque potrebbe mandarmi messaggi sapendo che solo io posso leggerli.

Problema

Le due chiavi sono interdipendenti ma deve essere **estremamente** difficile ricavare una chiave dall'altra.
(Leggasi: occorre provarle tutte)

Crittografia a chiave asimmetrica

Due chiavi - RSA

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

RSA

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

RSA

- Cifrario che prende il nome dalle iniziali dei tre creatori (Rivest, Shamir, Adleman)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

RSA

- Cifrario che prende il nome dalle iniziali dei tre creatori (Rivest, Shamir, Adleman)
- Pubblicato nel 1976

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

RSA

- Cifrario che prende il nome dalle iniziali dei tre creatori (Rivest, Shamir, Adleman)
- Pubblicato nel 1976
- Utilizza le proprietà dei numeri primi e dell'aritmetica modulare.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

RSA

- Cifrario che prende il nome dalle iniziali dei tre creatori (Rivest, Shamir, Adleman)
- Pubblicato nel 1976
- Utilizza le proprietà dei numeri primi e dell'aritmetica modulare.
- Non è possibile ricavare una chiave privata dalla chiave pubblica senza risolvere il problema della fattorizzazione in numeri primi del modulo RSA (un numero che è il prodotto di due numeri primi molto grandi ed è parte integrante dell'algoritmo di cifratura).

Crittografia a chiave asimmetrica

Due chiavi - RSA

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

RSA (continua)

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

RSA (continua)

- La generazione delle chiavi è *esplicitamente* onerosa per rallentare eventuali attacchi a forza bruta.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

RSA (continua)

- La generazione delle chiavi è *esplicitamente* onerosa per rallentare eventuali attacchi a forza bruta.
- Difficile da implementare efficentemente in hardware.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

RSA (continua)

- La generazione delle chiavi è *esplicitamente* onerosa per rallentare eventuali attacchi a forza bruta.
- Difficile da implementare efficentemente in hardware.
- Utilizzato principalmente per autenticare i soggetti coinvolti e per scambiare una chiave da utilizzare con un cifrario a chiave simmetrica.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Supponiamo di aver bisogno associare ad un file o ad un messaggio arbitrario un singolo numero.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Supponiamo di aver bisogno associare ad un file o ad un messaggio arbitrario un singolo numero.
Una funzione di hashing (o semplicemente hash) fa proprio questo: converte un messaggio in un numero.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Supponiamo di aver bisogno associare ad un file o ad un messaggio arbitrario un singolo numero.
Una funzione di hashing (o semplicemente hash) fa proprio questo: converte un messaggio in un numero.

Esempi di funzioni hash

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Supponiamo di aver bisogno associare ad un file o ad un messaggio arbitrario un singolo numero.
Una funzione di hashing (o semplicemente hash) fa proprio questo: converte un messaggio in un numero.

Esempi di funzioni hash

- $h_n(M) = M \bmod n$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Supponiamo di aver bisogno associare ad un file o ad un messaggio arbitrario un singolo numero.
Una funzione di hashing (o semplicemente hash) fa proprio questo: converte un messaggio in un numero.

Esempi di funzioni hash

- $h_n(M) = M \bmod n$
- Troncamento all'ultimo blocco.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash

Supponiamo di aver bisogno associare ad un file o ad un messaggio arbitrario un singolo numero.
Una funzione di hashing (o semplicemente hash) fa proprio questo: converte un messaggio in un numero.

Esempi di funzioni hash

- $h_n(M) = M \bmod n$
- Troncamento all'ultimo blocco.
- Checksum: $cs(M) = -1 \cdot \sum m_i$

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash (utilizzi)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash (utilizzi)

Le funzioni hash possono avere due utilizzi:

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash (utilizzi)

Le funzioni hash possono avere due utilizzi:

- Fornire l'indice per una tabella hash.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash (utilizzi)

Le funzioni hash possono avere due utilizzi:

- Fornire l'indice per una tabella hash.
- Stabilire se un messaggio è stato alterato o meno.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Funzioni hash (utilizzi)

Le funzioni hash possono avere due utilizzi:

- Fornire l'indice per una tabella hash.
- Stabilire se un messaggio è stato alterato o meno.

Le funzioni presentate prima non sono sufficientemente robuste per questo secondo scopo.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Hash crittografici (requisiti)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (requisiti)

Data una funzione hash H:

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (requisiti)

Data una funzione hash H:

1. Noto un hash $h = H(m)$ deve essere difficile risalire al messaggio m che ha generato h.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (requisiti)

Data una funzione hash H:

1. Noto un hash $h = H(m)$ deve essere difficile risalire al messaggio m che ha generato h.
2. Dato m_1 deve essere estremamente difficile trovare m_2 tale per cui $H(m_1) = H(m_2)$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (requisiti)

Data una funzione hash H:

1. Noto un hash $h = H(m)$ deve essere difficile risalire al messaggio m che ha generato h.
2. Dato m_1 deve essere estremamente difficile trovare m_2 tale per cui $H(m_1) = H(m_2)$
3. Dati m_1 ed m_2 distinti e diversi deve essere estremamente difficile che $H(m_1) = H(m_2)$

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (requisiti)

Data una funzione hash H:

1. Noto un hash $h = H(m)$ deve essere difficile risalire al messaggio m che ha generato h.
2. Dato m_1 deve essere estremamente difficile trovare m_2 tale per cui $H(m_1) = H(m_2)$
3. Dati m_1 ed m_2 distinti e diversi deve essere estremamente difficile che $H(m_1) = H(m_2)$

Le funzioni presentate prima falliscono i punti 2 e 3.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (esempi)

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (esempi)

- 1991 - MD5 (insicuro perché dal 2006 è possibile trovare collisioni in 60 secondi).

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (esempi)

- 1991 - MD5 (insicuro perché dal 2006 è possibile trovare collisioni in 60 secondi).
- 1993 - SHA-0 (ideato dalla NSA e subito ritirato perché dichiarato insicuro dalla stessa NSA).

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (esempi)

- 1991 - MD5 (insicuro perché dal 2006 è possibile trovare collisioni in 60 secondi).
- 1993 - SHA-0 (ideato dalla NSA e subito ritirato perché dichiarato insicuro dalla stessa NSA).
- 1993 - SHA-1 (nel febbraio 2017 Google ha trovato una collisione in due PDF).

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (esempi)

- 1991 - MD5 (insicuro perché dal 2006 è possibile trovare collisioni in 60 secondi).
- 1993 - SHA-0 (ideato dalla NSA e subito ritirato perché dichiarato insicuro dalla stessa NSA).
- 1993 - SHA-1 (nel febbraio 2017 Google ha trovato una collisione in due PDF).
- 2001 - SHA-2 (famiglia di algoritmi ideata dalla NSA, i due più usati sono SHA-256 e SHA-512 i cui nomi derivano dalla lunghezza in bit dell'hash).

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Hash crittografici (esempi)

- 1991 - MD5 (insicuro perché dal 2006 è possibile trovare collisioni in 60 secondi).
- 1993 - SHA-0 (ideato dalla NSA e subito ritirato perché dichiarato insicuro dalla stessa NSA).
- 1993 - SHA-1 (nel febbraio 2017 Google ha trovato una collisione in due PDF).
- 2001 - SHA-2 (famiglia di algoritmi ideata dalla NSA, i due più usati sono SHA-256 e SHA-512 i cui nomi derivano dalla lunghezza in bit dell'hash).
- 2015 - SHA-3 (famiglia di algoritmi non ideati dalla NSA, vincitori di una competizione per trovare i successori di SHA-2).

Hash e firma crittografica

Firma crittografica

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Domanda

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Domanda

Un hash è criptabile. Che succede se compilo un hash crittografico del mio messaggio trasmesso in chiaro e cripto l'hash con la mia chiave privata?

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Domanda

Un hash è criptabile. Che succede se compilo un hash crittografico del mio messaggio trasmesso in chiaro e cripto l'hash con la mia chiave privata?

Risposta

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Domanda

Un hash è criptabile. Che succede se compilo un hash crittografico del mio messaggio trasmesso in chiaro e cripto l'hash con la mia chiave privata?

Risposta

Chiunque sia in possesso della mia chiave pubblica può decrittare l'hash e verificare che corrisponda a quello che si ottiene dal testo in chiaro.

Introduzione alla crittografia
Gianfranco Gallizia
Introduzione
Un po' di storia
Crittografia a chiave simmetrica
Crittografia a chiave asimmetrica
Hash e firma crittografica
Conclusioni

Domanda

Un hash è criptabile. Che succede se compilo un hash crittografico del mio messaggio trasmesso in chiaro e cripto l'hash con la mia chiave privata?

Risposta

Chiunque sia in possesso della mia chiave pubblica può decrittare l'hash e verificare che corrisponda a quello che si ottiene dal testo in chiaro.

Benefici

Hash e firma crittografica

Firma crittografica

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Domanda

Un hash è criptabile. Che succede se compilo un hash crittografico del mio messaggio trasmesso in chiaro e cripto l'hash con la mia chiave privata?

Risposta

Chiunque sia in possesso della mia chiave pubblica può decrittare l'hash e verificare che corrisponda a quello che si ottiene dal testo in chiaro.

Benefici

Il messaggio è autenticato: solo io posso aver criptato in quella maniera l'hash e il destinatario ha la garanzia (data dalla funzione hash scelta) che il mio messaggio non è stato alterato.

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Principio di Kerckhoffs

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Principio di Kerckhoffs

La sicurezza di un sistema crittografico dipende unicamente dalla sicurezza della chiave.

Conclusioni

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Principio di Kerckhoffs

La sicurezza di un sistema crittografico dipende unicamente dalla sicurezza della chiave.

Massima di Shannon

Il nemico conosce il sistema.

Introduzione alla crittografia

Gianfranco Gallizia

Introduzione

Un po' di storia

Crittografia a chiave simmetrica

Crittografia a chiave asimmetrica

Hash e firma crittografica

Conclusioni

Grazie per l'attenzione.
Domande ?