Controllo, privacy, crittografia

Gabriele Vanoni[1][2]

16 Febbraio 2016,
Liceo Zucchi, Monza

[1]Politecnico di Milano
[2]Lab61

Indice

Un esperimento

La lezione di oggi è un esperimento per vari motivi.

Un esperimento

La lezione di oggi è un esperimento per vari motivi.

- Non ho mai parlato pubblicamente a degli studenti delle scuole superiori.

Un esperimento

La lezione di oggi è un esperimento per vari motivi.

- Non ho mai parlato pubblicamente a degli studenti delle scuole superiori.
- Non ho mai parlato pubblicamente di sociologia, non essendo il mio ambito di studio.

Un esperimento

La lezione di oggi è un esperimento per vari motivi.

- Non ho mai parlato pubblicamente a degli studenti delle scuole superiori.
- Non ho mai parlato pubblicamente di sociologia, non essendo il mio ambito di studio.
- Ho provato a mettere insieme temi scientifici a temi filosofici e sociologici.

Un esperimento

La lezione di oggi è un esperimento per vari motivi.

- Non ho mai parlato pubblicamente a degli studenti delle scuole superiori.
- Non ho mai parlato pubblicamente di sociologia, non essendo il mio ambito di studio.
- Ho provato a mettere insieme temi scientifici a temi filosofici e sociologici.
- Seguirò un percorso inverso a quello che sembrerebbe più logico, perché voglio avervi svegli sulla matematica.

Informatica, algoritmi e crittografia

Informatica

"Computer science is no more about computers than astronomy is about telescopes"

Edsger Dijkstra

Informatica

"Computer science is no more about computers than astronomy is about telescopes"

Edsger Dijkstra

"I shall be sorry if computer science ever flies apart into two disciplines, one logical and one technological"

Robin Milner

Informatica

"Computer science is no more about computers than astronomy is about telescopes"

Edsger Dijkstra

"I shall be sorry if computer science ever flies apart into two disciplines, one logical and one technological"

Robin Milner

"Il padre dell'informatica è l'ingegneria, ma la madre è la logica"

Maria Emilia Maietti

Un problema anche linguistico

- In italiano il termine informatica è omnicomprensivo. In inglese esistono due differenti locuzioni: **computer science** e **information technology**.

Un problema anche linguistico

- In italiano il termine informatica è omnicomprensivo. In inglese esistono due differenti locuzioni: **computer science** e **information technology**.
- Storicamente l'informatica nasce nei dipartimenti di **matematica** delle università, venti anni prima della creazione del primo calcolatore elettronico.

Un problema anche linguistico

- In italiano il termine informatica è omnicomprensivo. In inglese esistono due differenti locuzioni: **computer science** e **information technology**.
- Storicamente l'informatica nasce nei dipartimenti di **matematica** delle università, venti anni prima della creazione del primo calcolatore elettronico.
- Quando si comincia la costruzione dei calcolatori allora entrano in campo gli **ingegneri**.

Un problema anche linguistico

- In italiano il termine informatica è omnicomprensivo. In inglese esistono due differenti locuzioni: **computer science** e **information technology**.
- Storicamente l'informatica nasce nei dipartimenti di **matematica** delle università, venti anni prima della creazione del primo calcolatore elettronico.
- Quando si comincia la costruzione dei calcolatori allora entrano in campo gli **ingegneri**.
- Oggi anche chi fa un sito web è considerato un informatico.

Un problema anche linguistico

- In italiano il termine informatica è omnicomprensivo. In inglese esistono due differenti locuzioni: **computer science** e **information technology**.
- Storicamente l'informatica nasce nei dipartimenti di **matematica** delle università, venti anni prima della creazione del primo calcolatore elettronico.
- Quando si comincia la costruzione dei calcolatori allora entrano in campo gli **ingegneri**.
- Oggi anche chi fa un sito web è considerato un informatico.
- Ci occuperemo (molto brevemente) della nozione chiave dell'informatica, quella di **algoritmo**.

Che cos'è un algoritmo?

Dare una definizione precisa e rigorosa è difficile (ma si può, anche in diversi termini) e ci ritorniamo dopo.

Che cos'è un algoritmo?

Dare una definizione precisa e rigorosa è difficile (ma si può, anche in diversi termini) e ci ritorniamo dopo.
Il termine è sulla bocca di tutti: solo l'altro giorno si parlava dell'algoritmo sbagliato per il calcolo delle tariffe degli abbonamenti del treno.

Che cos'è un algoritmo?

Dare una definizione precisa e rigorosa è difficile (ma si può, anche in diversi termini) e ci ritorniamo dopo.
Il termine è sulla bocca di tutti: solo l'altro giorno si parlava dell'algoritmo sbagliato per il calcolo delle tariffe degli abbonamenti del treno.

Intuitivamente sapete indicarmi degli esempi e descrivermi il loro funzionamento?

Che cos'è un algoritmo?

Dare una definizione precisa e rigorosa è difficile (ma si può, anche in diversi termini) e ci ritorniamo dopo.
Il termine è sulla bocca di tutti: solo l'altro giorno si parlava dell'algoritmo sbagliato per il calcolo delle tariffe degli abbonamenti del treno.

Intuitivamente sapete indicarmi degli esempi e descrivermi il loro funzionamento?

Possiamo quindi dire informalmente che un **algoritmo** è una procedura che dato un **input** restituisce un **output**, utilizzando un **numero finito** di **regole**.

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.
La misura di efficienza di un algoritmo si chiama **complessità computazionale**.

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.
La misura di efficienza di un algoritmo si chiama **complessità computazionale**.
Normalmente viene espressa come una funzione della **dimensione** dell'**input**. Per esempio $C = n$, $C = n^2$, $C = 2^n$. (Trascuro i dettagli della notazione O-grande).

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.
La misura di efficienza di un algoritmo si chiama **complessità computazionale**.
Normalmente viene espressa come una funzione della **dimensione** dell'**input**. Per esempio $C = n$, $C = n^2$, $C = 2^n$. (Trascuro i dettagli della notazione O-grande).

Esempi

- Ricerca binaria.

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.
La misura di efficienza di un algoritmo si chiama **complessità computazionale**.
Normalmente viene espressa come una funzione della **dimensione** dell'**input**. Per esempio $C = n$, $C = n^2$, $C = 2^n$. (Trascuro i dettagli della notazione O-grande).

Esempi

- Ricerca binaria.
- La somma in colonna.

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.
La misura di efficienza di un algoritmo si chiama **complessità computazionale**.
Normalmente viene espressa come una funzione della **dimensione** dell'**input**. Per esempio $C = n$, $C = n^2$, $C = 2^n$. (Trascuro i dettagli della notazione O-grande).

Esempi

- Ricerca binaria.
- La somma in colonna.
- Un algoritmo di ordinamento.

La complessità degli algoritmi

In genere si è interessati a trovari **algoritmi efficienti**, veloci per risolvere i problemi.
La misura di efficienza di un algoritmo si chiama **complessità computazionale**.
Normalmente viene espressa come una funzione della **dimensione** dell'**input**. Per esempio $C = n$, $C = n^2$, $C = 2^n$. (Trascuro i dettagli della notazione O-grande).

Esempi

- Ricerca binaria.
- La somma in colonna.
- Un algoritmo di ordinamento.
- Il problema del commesso viaggiatore.

La comunicazione

Definizione

Definiamo un modello di comunicazione:
Sorgente (S) - **Canale** (C) - **Destinazione** (D).
Il **messaggio** per arrivare da S a D transita per C.

La comunicazione

Definizione

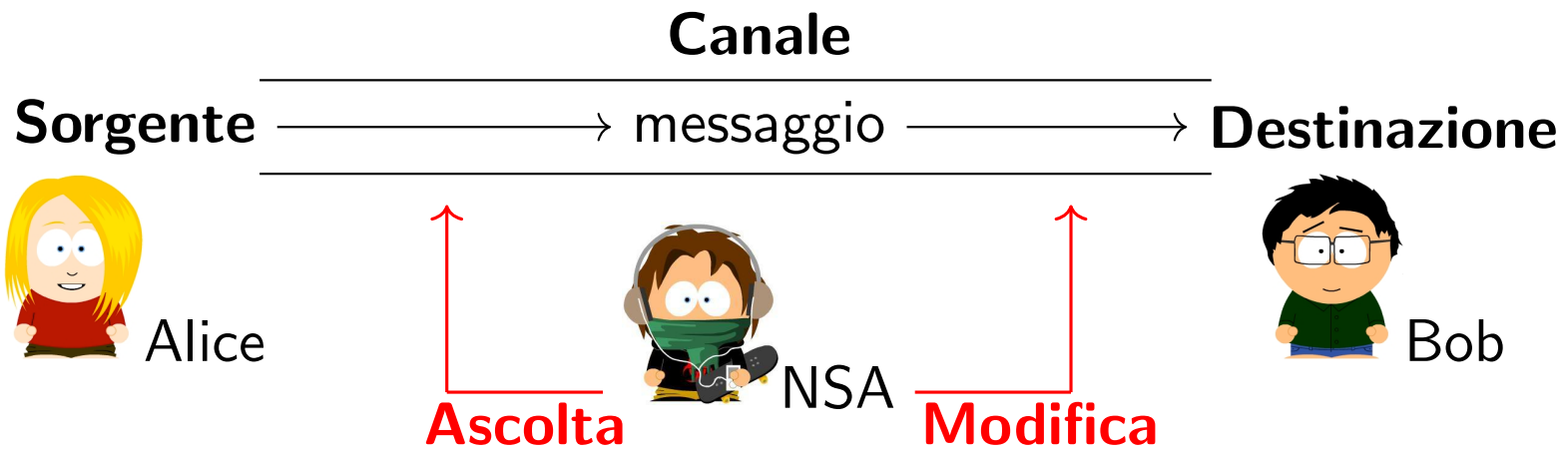
Definiamo un modello di comunicazione:
Sorgente (S) - **Canale** (C) - **Destinazione** (D).
Il **messaggio** per arrivare da S a D transita per C.

La necessità della sicurezza

Quando comunichiamo spesso necessitiamo di certe proprietà di **sicurezza**.

La necessità della sicurezza

Quando comunichiamo spesso necessitiamo di certe proprietà di **sicurezza**.



Le proprietà fondamentali (1)

Confidenzialità

Definizione

È la proprietà che assicura che il messaggio non venga compreso da un utente esterno mentre transita nel canale.

Le proprietà fondamentali (1)

Confidenzialità

Definizione

È la proprietà che assicura che il messaggio non venga compreso da un utente esterno mentre transita nel canale.

Autenticità

Definizione

È la proprietà che assicura che il messaggio sia stato spedito realmente da chi ci aspettiamo che l'abbia spedito.

Le proprietà fondamentali (2)

Disponibilità

Definizione

È la proprietà che assicura che una volta arrivato, il messaggio sia subito disponibile.

Le proprietà fondamentali (2)

Disponibilità

Definizione

È la proprietà che assicura che una volta arrivato, il messaggio sia subito disponibile.

Integrità

Definizione

È la proprità che ci assicura che il messaggio non sia cambiato dal momento dell'invio a quello della ricezione, ovvero durante il transito nel canale.

Soluzioni? (1)

Soluzione banale

Non comunico.

Soluzioni? (1)

Soluzione banale

Non comunico.

Spesso è la maniera migliore di risolvere il problema, rimuovendo il messaggio rimuovo anche il pericolo che altri lo conoscano.

Soluzioni? (1)

Soluzione banale

Non comunico.

Spesso è la maniera migliore di risolvere il problema, rimuovendo il messaggio rimuovo anche il pericolo che altri lo conoscano.

Soluzione meno banale

Nascondo il messaggio.

Soluzioni? (1)

Soluzione banale

Non comunico.

Spesso è la maniera migliore di risolvere il problema, rimuovendo il messaggio rimuovo anche il pericolo che altri lo conoscano.

Soluzione meno banale

Nascondo il messaggio.

È una soluzione praticabile e praticata, chiamata **steganografia**. I messaggi possono ad esempio essere nascosti in immagini o occultati nei modi più diversi.

Soluzioni? (2)

Soluzione naïve

Blindare il canale.

Soluzioni? (2)

Soluzione naïve

Blindare il canale.

È una soluzione chiaramente inattuabile data la natura di internet. Internet è infatti una **rete distribuita** e i messaggi passano da molti intermediari prima di arrivare a destinazione.

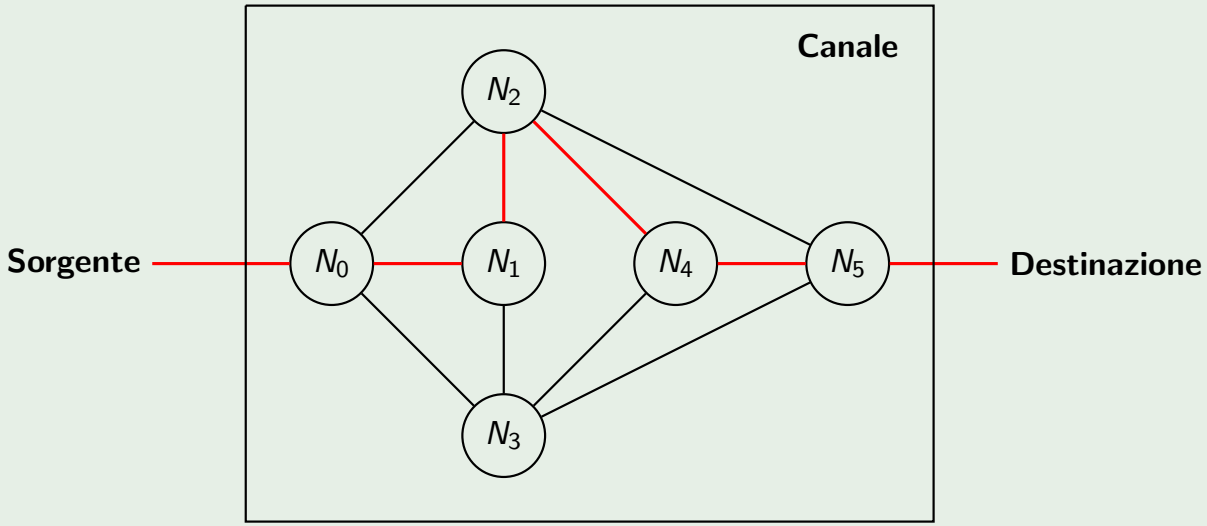
Soluzioni? (2)

Soluzione naïve

Blindare il canale.

È una soluzione chiaramente inattuabile data la natura di internet. Internet è infatti una **rete distribuita** e i messaggi passano da molti intermediari prima di arrivare a destinazione.

Esempio

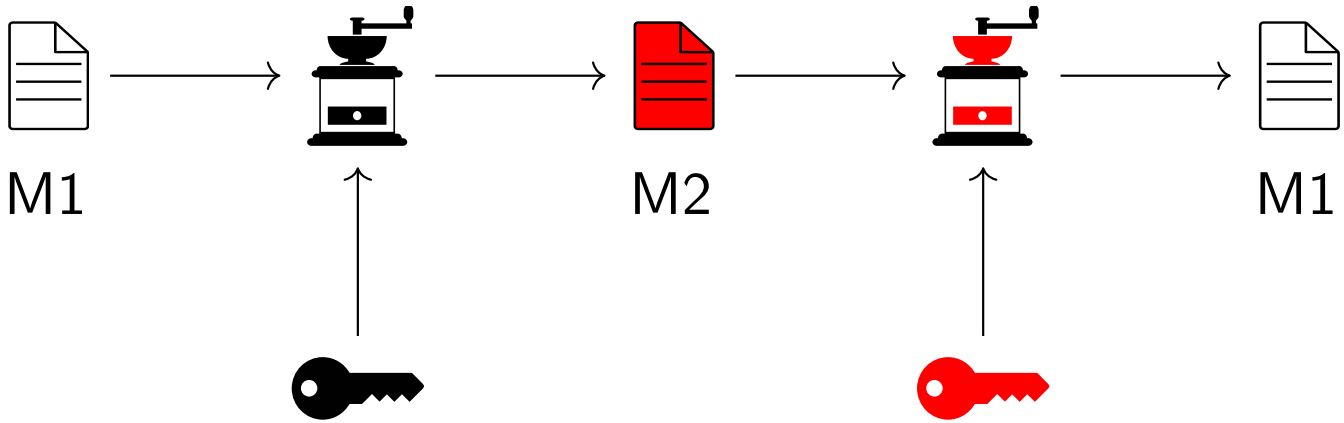


L'idea della crittografia

Perciò nasce l'idea della crittografia, ovvero un meccanismo che permette di trasformare il messaggio M1 in un altro altro M2, incomprensibile per chiunque, e che solo il possessore della chiave potrà ritrasformare in quello originale M1.

L'idea della crittografia

Perciò nasce l'idea della crittografia, ovvero un meccanismo che permette di trasformare il messaggio M1 in un altro altro M2, incomprensibile per chiunque, e che solo il possessore della chiave potrà ritrasformare in quello originale M1.



Formalmente

Definizione

Un **crittosistema** Ξ è una quintupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ dove:

- $\mathcal{P}$ è l'insieme dei messaggi in chiaro,
- $\mathcal{C}$ è l'insieme dei messaggi cifrati,
- $\mathcal{K}$ è l'insieme delle chiavi,
- $\mathcal{E} = \{E_k | \, k \in \mathcal{K}\}$ è la famiglia di funzioni di cifratura iniettive tale che $E_k : \mathcal{P} \to \mathcal{C}$ per ogni $k \in \mathcal{K}$,
- $\mathcal{D} = \{D_k | \, k \in \mathcal{K}\}$ è la famiglia di funzioni di decifratura biiettive tale che $D_k : \mathcal{C} \to \mathcal{P}$ per ogni $k \in \mathcal{K}$,

tale che per ogni $e \in \mathcal{K}$ esiste unica $d \in \mathcal{K}$ tale $D_d(E_e(m)) = m$, per ogni $m \in \mathcal{P}$.

Le tecniche

Esistono fondamentalmente due diversi meccanismi di cifratura: a **chiave pubblica** e a **chiave privata** che a loro volta si basano su diversi tipi di **algoritmi**.

Crittografia simmetrica	**Crittografia asimmetrica**
DES	Diffie-Hellman
3DES	Curve ellittiche
AES	RSA
...	...

Gli algoritmi che permettono l'effettivo funzionamento della crittografia si basano su della matematica parecchio avanzata e in particolare sulla teoria dei numeri, sull'algebra (tipicamente dei campi finiti), sulla teoria della probabilità e sulla teoria della complessità computazionale.

Crittografia simmetrica

Definizione

La **crittografia simmetrica** è un meccanismo che utilizza la stessa chiave per cifrare e decifrare il messaggio.

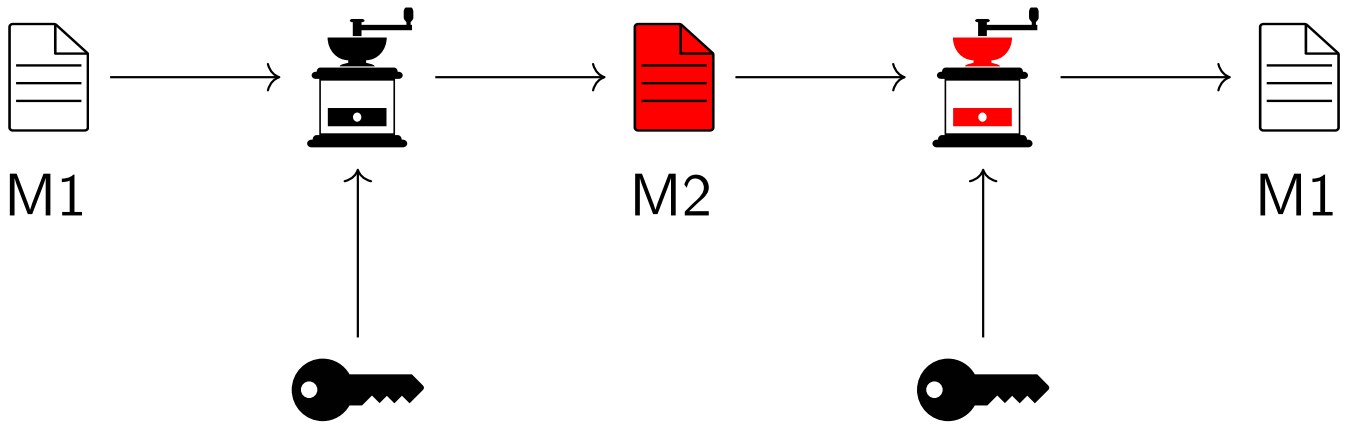
Formalmente $D_k(E_k(m)) = m$ per ogni $m \in \mathcal{P}$ e per ogni $k \in \mathcal{K}$, con D_k e E_k semplici (veloci) da calcolare.

Crittografia simmetrica

Definizione

La **crittografia simmetrica** è un meccanismo che utilizza la stessa chiave per cifrare e decifrare il messaggio.

Formalmente $D_k(E_k(m)) = m$ per ogni $m \in \mathcal{P}$ e per ogni $k \in \mathcal{K}$, con D_k e E_k semplici (veloci) da calcolare.



Problema!

E lo scambio della chiave?

Problema!

E lo scambio della chiave?

Nella crittografia simmetrica sia il mittente che il ricevente devono conoscere la chiave, cioè devono essersela scambiata in qualche momento. A questo punto però lo scambio della chiave come fa ad avvenire in maniera sicura? Se utilizzassimo di nuovo un metodo di cifratura simmetrico per cifrare la chiave saremmo al punto di partenza.

Problema!

E lo scambio della chiave?

Nella crittografia simmetrica sia il mittente che il ricevente devono conoscere la chiave, cioè devono essersela scambiata in qualche momento. A questo punto però lo scambio della chiave come fa ad avvenire in maniera sicura? Se utilizzassimo di nuovo un metodo di cifratura simmetrico per cifrare la chiave saremmo al punto di partenza.

Per questo tipicamente o si utilizza per scambiare la chiave un altro canale considerato sicuro oppure si ricorre alla...

Crittografia asimmetrica

Definizione

La **crittografia asimmetrica** è un meccanismo che funziona con due chiavi. Se si cifra il messaggio con la prima, con la seconda lo si decifra e viceversa.

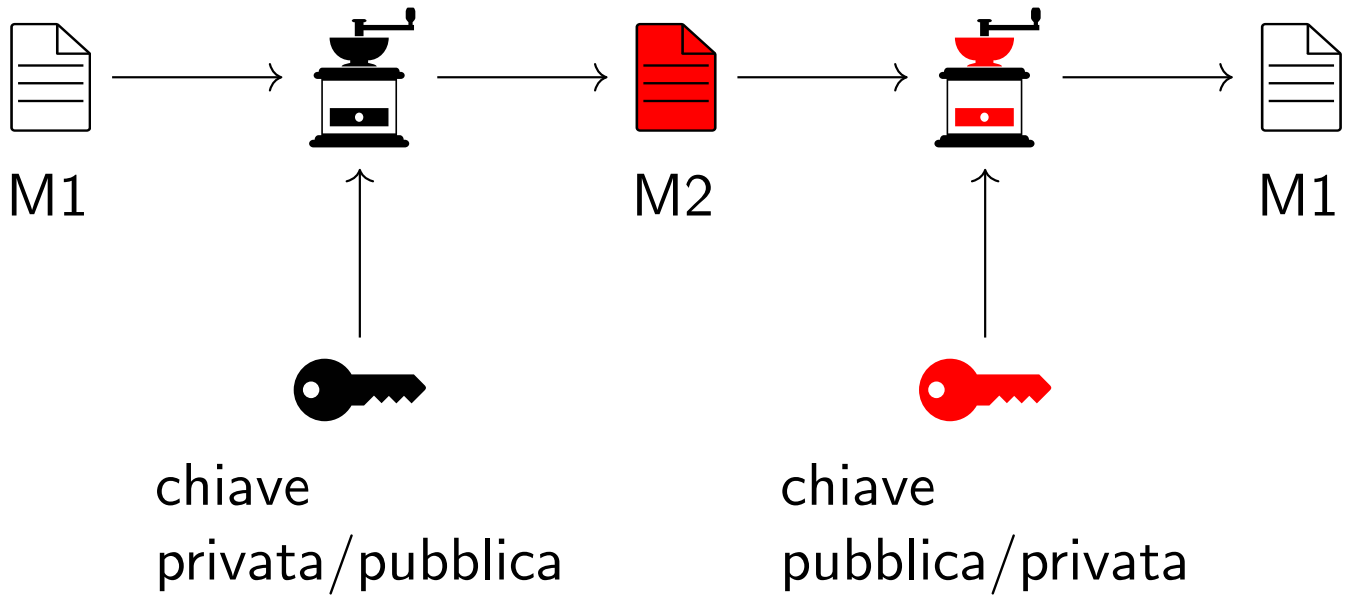
In realtà non è così, ma possiamo immaginarlo in questo modo.

Crittografia asimmetrica

Definizione

La **crittografia asimmetrica** è un meccanismo che funziona con due chiavi. Se si cifra il messaggio con la prima, con la seconda lo si decifra e viceversa.

In realtà non è così, ma possiamo immaginarlo in questo modo.



Dogma della crittografia asimmetrica

La seguente regola è sempre da rispettare quando si utilizza un **sistema crittografico asimmetrico**.

Dogma della crittografia asimmetrica

La seguente regola è sempre da rispettare quando si utilizza un **sistema crittografico asimmetrico**.

Dogma

Ogni utente deve mantenere segreta una delle chiavi, che chiameremo **privata** e distribuire l'altra, che chiameremo **pubblica**.

Funzionamento nella comunicazione - confidenzialità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **confidenzialità**.
Per la comunicazione bisogna seguire questi passaggi:

Funzionamento nella comunicazione - confidenzialità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **confidenzialità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione confidenziale

1° passo: cifro il messaggio con la chiave pubblica del destinatario.

Funzionamento nella comunicazione - confidenzialità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **confidenzialità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione confidenziale

1° passo: cifro il messaggio con la chiave pubblica del destinatario.
2° passo: invio il messaggio cifrato.

Funzionamento nella comunicazione - confidenzialità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **confidenzialità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione confidenziale

1° passo: cifro il messaggio con la chiave pubblica del destinatario.
2° passo: invio il messaggio cifrato.
3° passo: il destinatario lo decifra con la sua chiave privata.

Funzionamento nella comunicazione - confidenzialità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **confidenzialità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione confidenziale

1° passo: cifro il messaggio con la chiave pubblica del destinatario.
2° passo: invio il messaggio cifrato.
3° passo: il destinatario lo decifra con la sua chiave privata.

In questa maniera mentre il messaggio transita nel canale il messaggio è cifrato e solo chi è in possesso della chiave privata corrispondente a quella pubblica con cui è stato cifrato potrà decrittarlo.

Funzionamento nella comunicazione - autenticità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **autenticità**.
Per la comunicazione bisogna seguire questi passaggi:

Funzionamento nella comunicazione - autenticità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **autenticità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione autentica

1° passo: cifro il messaggio con la mia chiave privata.

Funzionamento nella comunicazione - autenticità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **autenticità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione autentica

1° passo: cifro il messaggio con la mia chiave privata.
2° passo: invio il messaggio cifrato.

Funzionamento nella comunicazione - autenticità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **autenticità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione autentica

1° passo: cifro il messaggio con la mia chiave privata.
2° passo: invio il messaggio cifrato.
3° passo: il destinatario lo decifra con la mia chiave pubblica.

Funzionamento nella comunicazione - autenticità

Vediamo ora come utilizzare la **crittografia asimmetrica** per ottenere la proprietà di **autenticità**.
Per la comunicazione bisogna seguire questi passaggi:

Protocollo per la comunicazione autentica

1° passo: cifro il messaggio con la mia chiave privata.
2° passo: invio il messaggio cifrato.
3° passo: il destinatario lo decifra con la mia chiave pubblica.

In questa maniera il destinatario è sicuro che il mittente sia proprio chi deve essere (ha infatti utilizzato la propria chiave privata) perché altrimenti non riuscirebbe a decrittare il messaggio con la sua chiave pubblica.

Conclusioni

Non abbiamo parlato della **disponiblità** e dell'**integrità**.

Conclusioni

Non abbiamo parlato della **disponiblità** e dell'**integrità**.

La prima è assicurata dal fatto che operazioni di decrittazione sono "veloci".

Conclusioni

Non abbiamo parlato della **disponiblità** e dell'**integrità**.
La prima è assicurata dal fatto che operazioni di decrittazione sono "veloci".
Per l'**integrità** si può utilizzare uno dei tanti protocolli che calcolano l'**hash** di un testo, ovvero una "impronta digitale". Inviando insieme al testo anche l'hash il destinatario potrà ricalcolare l'hash sul testo arrivato e confrontarlo con quello arrivato. Se coincidono c'è un'altissima probabilità che il testo sia integro, se non coincidono certamente il testo arrivato è diverso da quello spedito.

Conclusioni

Non abbiamo parlato della **disponiblità** e dell'**integrità**.
La prima è assicurata dal fatto che operazioni di decrittazione sono "veloci".
Per l'**integrità** si può utilizzare uno dei tanti protocolli che calcolano l'**hash** di un testo, ovvero una "impronta digitale". Inviando insieme al testo anche l'hash il destinatario potrà ricalcolare l'hash sul testo arrivato e confrontarlo con quello arrivato. Se coincidono c'è un'altissima probabilità che il testo sia integro, se non coincidono certamente il testo arrivato è diverso da quello spedito.
Esempi di protocolli di hash sono **SHA** e **MD5**.

Controllo e privacy
(basato sul lavoro di tesi di Paolo Andreozzi)

Niente da nascondere

If you have nothing to hide, you've nothing to fear.

Niente da nascondere

If you have nothing to hide, you've nothing to fear.

- Questo è l'**argomento** principale portato avanti da tutti coloro che provano attraverso proposte di legge a minare il diritto alla **privacy** e alla **riservatezza**.

Niente da nascondere

If you have nothing to hide, you've nothing to fear.

- Questo è l'**argomento** principale portato avanti da tutti coloro che provano attraverso proposte di legge a minare il diritto alla **privacy** e alla **riservatezza**.
- L'argomento è centrale perché mette in relazione il piano **individuale** con il piano **statale**.

Niente da nascondere

If you have nothing to hide, you've nothing to fear.

- Questo è l'**argomento** principale portato avanti da tutti coloro che provano attraverso proposte di legge a minare il diritto alla **privacy** e alla **riservatezza**.
- L'argomento è centrale perché mette in relazione il piano **individuale** con il piano **statale**.
- Inizialmente infatti quando parliamo di **controllo** ci riferiremo a quello dello **stato**.

Un corollario

Direttamente dall'argomento *Nothing to hide* discende l'equazione:

nascosto = sbagliato

Un corollario

Direttamente dall'argomento *Nothing to hide* discende l'equazione:

nascosto = sbagliato

Perciò nel 1978 il governo degli Stati Uniti d'America emette all'interno del *Foreign Intelligence Surveillance Act* degli articoli che autorizzano l'**NSA** a collezionare e archiviare informazioni raccolte nel corso di comunicazioni, semplicemente per il fatto che siano cifrate, per il tempo necessario alla loro decrittazione.

Un corollario

Direttamente dall'argomento *Nothing to hide* discende l'equazione:

nascosto = sbagliato

Perciò nel 1978 il governo degli Stati Uniti d'America emette all'interno del *Foreign Intelligence Surveillance Act* degli articoli che autorizzano l'**NSA** a collezionare e archiviare informazioni raccolte nel corso di comunicazioni, semplicemente per il fatto che siano cifrate, per il tempo necessario alla loro decrittazione.
Addirittura le *International Traffic in Arms Regulations* previste dall'*Arms Export Act* del 1978 includono nell'elenco delle **armi** sottoposte a disciplina la **crittografia**.

Un corollario

Direttamente dall'argomento *Nothing to hide* discende l'equazione:

nascosto = sbagliato

Perciò nel 1978 il governo degli Stati Uniti d'America emette all'interno del *Foreign Intelligence Surveillance Act* degli articoli che autorizzano l'**NSA** a collezionare e archiviare informazioni raccolte nel corso di comunicazioni, semplicemente per il fatto che siano cifrate, per il tempo necessario alla loro decrittazione.
Addirittura le *International Traffic in Arms Regulations* previste dall'*Arms Export Act* del 1978 includono nell'elenco delle **armi** sottoposte a disciplina la **crittografia**. Ci sono disposizioni di sistemi penali come quello indiano, inglese, francese o sudafricano che attualmente puniscono penalmente chi rifiuti di consegnare password e chiavi di cifratura quando richiesto dalle autorità.

Un corollario

Direttamente dall'argomento *Nothing to hide* discende l'equazione:

nascosto = sbagliato

Perciò nel 1978 il governo degli Stati Uniti d'America emette all'interno del *Foreign Intelligence Surveillance Act* degli articoli che autorizzano l'**NSA** a collezionare e archiviare informazioni raccolte nel corso di comunicazioni, semplicemente per il fatto che siano cifrate, per il tempo necessario alla loro decrittazione.
Addirittura le *International Traffic in Arms Regulations* previste dall'*Arms Export Act* del 1978 includono nell'elenco delle **armi** sottoposte a disciplina la **crittografia**. Ci sono disposizioni di sistemi penali come quello indiano, inglese, francese o sudafricano che attualmente puniscono penalmente chi rifiuti di consegnare password e chiavi di cifratura quando richiesto dalle autorità.
Limitazioni sono state poste da varie legislazioni alla lunghezza delle chiavi di sessione utilizzate.

Lo stato e la criminalizzazione

Partiamo dalla definizione di **Max Weber** che definisce lo **stato** come:

Lo stato e la criminalizzazione

Partiamo dalla definizione di **Max Weber** che definisce lo **stato** come:

> comunità umana che, entro un territorio definito [...] reclama per sé con successo il monopolio della forza legittima.

Lo stato e la criminalizzazione

Partiamo dalla definizione di **Max Weber** che definisce lo **stato** come:

> comunità umana che, entro un territorio definito [...] reclama per sé con successo il monopolio della forza legittima.

- Lo **stato** però non è solo questo. Secondo Bourdieu l'entità statale è in grado di definire **concetti** e **identità sociali**, crea quindi **categorie** e **condotte** e conduce a pensarle come naturali.

Lo stato e la criminalizzazione

Partiamo dalla definizione di **Max Weber** che definisce lo **stato** come:

> comunità umana che, entro un territorio definito [...] reclama per sé con successo il monopolio della forza legittima.

- Lo **stato** però non è solo questo. Secondo Bourdieu l'entità statale è in grado di definire **concetti** e **identità sociali**, crea quindi **categorie** e **condotte** e conduce a pensarle come naturali.
- Istituzionalizza **norme sociali** e in particolare criminalizza alcuni comportamenti facendoli entrare nel campo della sanzione penale.

Uscire dall'ambito giuridico

- L'attacco alla **privacy** è possibile perché lo stesso concetto di privacy viene considerato solo dal punto di vista **giuridico**.

Uscire dall'ambito giuridico

- L'attacco alla **privacy** è possibile perché lo stesso concetto di privacy viene considerato solo dal punto di vista **giuridico**.
- In questo ambito si utilizza il principio del "**bilanciamento dei diritti**". In questo caso i diritti da bilanciare sono quello alla **sicurezza** e quello alla **riservatezza** ed è facile convincersi che quello alla sicurezza abbia maggior forza.

Uscire dall'ambito giuridico

- L'attacco alla **privacy** è possibile perché lo stesso concetto di privacy viene considerato solo dal punto di vista **giuridico**.
- In questo ambito si utilizza il principio del "**bilanciamento dei diritti**". In questo caso i diritti da bilanciare sono quello alla **sicurezza** e quello alla **riservatezza** ed è facile convincersi che quello alla sicurezza abbia maggior forza.
- Risulta necessario quindi uscire dall'ambito prettamente giuridico (cioè statale) ed affermare che il diritto alla riservatezza è assolutamente naturale e ragionevole, un bisogno di tipo antropologico.

Il significato della privacy

La **privacy** è un **valore** fortemente interconnesso con (la **libertà** di esercitare) l'**autonomia**, l'**uguaglianza** e la **democrazia**.

Il significato della privacy

La **privacy** è un **valore** fortemente interconnesso con (la **libertà** di esercitare) l'**autonomia**, l'**uguaglianza** e la **democrazia**.

> Friendship, intimacy, and trust could not develop in societies or context in which individuals are under constant surveillance (Fried 1968)

Il significato della privacy

La **privacy** è un **valore** fortemente interconnesso con (la **libertà** di esercitare) l'**autonomia**, l'**uguaglianza** e la **democrazia**.

Friendship, intimacy, and trust could not develop in societies or context in which individuals are under constant surveillance (Fried 1968)

Privacy is necessary to maintain a diversity of relationships: the kind of relationships we have with others is a function of the information we have about each other; if everyone had the same information about you, you would not have a diversity of relationship (Rachels 1975)

Il significato della privacy

La **privacy** è un **valore** fortemente interconnesso con (la **libertà** di esercitare) l'**autonomia**, l'**uguaglianza** e la **democrazia**.

> Friendship, intimacy, and trust could not develop in societies or context in which individuals are under constant surveillance (Fried 1968)

> Privacy is necessary to maintain a diversity of relationships: the kind of relationships we have with others is a function of the information we have about each other; if everyone had the same information about you, you would not have a diversity of relationship (Rachels 1975)

Pensate al gossip!

Il significato della privacy

La **privacy** è un **valore** fortemente interconnesso con (la **libertà** di esercitare) l'**autonomia**, l'**uguaglianza** e la **democrazia**.

Friendship, intimacy, and trust could not develop in societies or context in which individuals are under constant surveillance (Fried 1968)

Privacy is necessary to maintain a diversity of relationships: the kind of relationships we have with others is a function of the information we have about each other; if everyone had the same information about you, you would not have a diversity of relationship (Rachels 1975)

Pensate al gossip!

Instead of framing privacy as an individual good, we should understand it as a social good (Regan 1995)

Dallo stato alle corporation allo stato

- Nel 1999 il CEO di Sun Microsystems, Scott McNealy dichiarò a una conferenza: “You have zero privacy anyway. Get over it.”, venendo investito da decine di critiche e attacchi.

Dallo stato alle corporation allo stato

- Nel 1999 il CEO di Sun Microsystems, Scott McNealy dichiarò a una conferenza: "You have zero privacy anyway. Get over it.", venendo investito da decine di critiche e attacchi.
- Undici anni dopo nel 2010 **Mark Zuckerberg** dichiara che la **privacy** non è più una norma sociale, senza suscitare alcuna reazione e apparendo la sua frase una mera constatazione.

Dallo stato alle corporation allo stato

- Nel 1999 il CEO di Sun Microsystems, Scott McNealy dichiarò a una conferenza: "You have zero privacy anyway. Get over it.", venendo investito da decine di critiche e attacchi.
- Undici anni dopo nel 2010 **Mark Zuckerberg** dichiara che la **privacy** non è più una norma sociale, senza suscitare alcuna reazione e apparendo la sua frase una mera constatazione.
- I grandi colossi di internet Google, Facebook, Twitter, Amazon, etc hanno accesso ad un'immensa mole di **dati** su cui basano il proprio **business**. Non si fanno però generalmente problemi a rilasciarli ai **governi** che li richiedono.

Temi correlati

- Motori di ricerca personalizzati (filter bubble)
- Pubblicità personalizzate
- Recommender systems
- Data mining e conseguente controllo
- Monopolio della crittografia e back-door

Riferimenti bibliografici

- http://web.math.unifi.it/users/fumagal/documenti/Crittografia_Capitoli1-6.pdf
- http://poisson.phc.unipi.it/~papini/TCC.pdf
- https://www.iacr.org/authors/tikz/
- https://thenounproject.com/ - Viktor Vorobyev, Apirat Ditsayarak, Guilhem
- Paolo Andreozzi, *Criminalizzare la crittografia: l'ingresso dello stato nelle spazialità cifrate* (E bibliografia ivi contenuta)
- Note della prof.ssa Schiaffonati per il corso di *Computer Ethics* al Politecnico di Milano