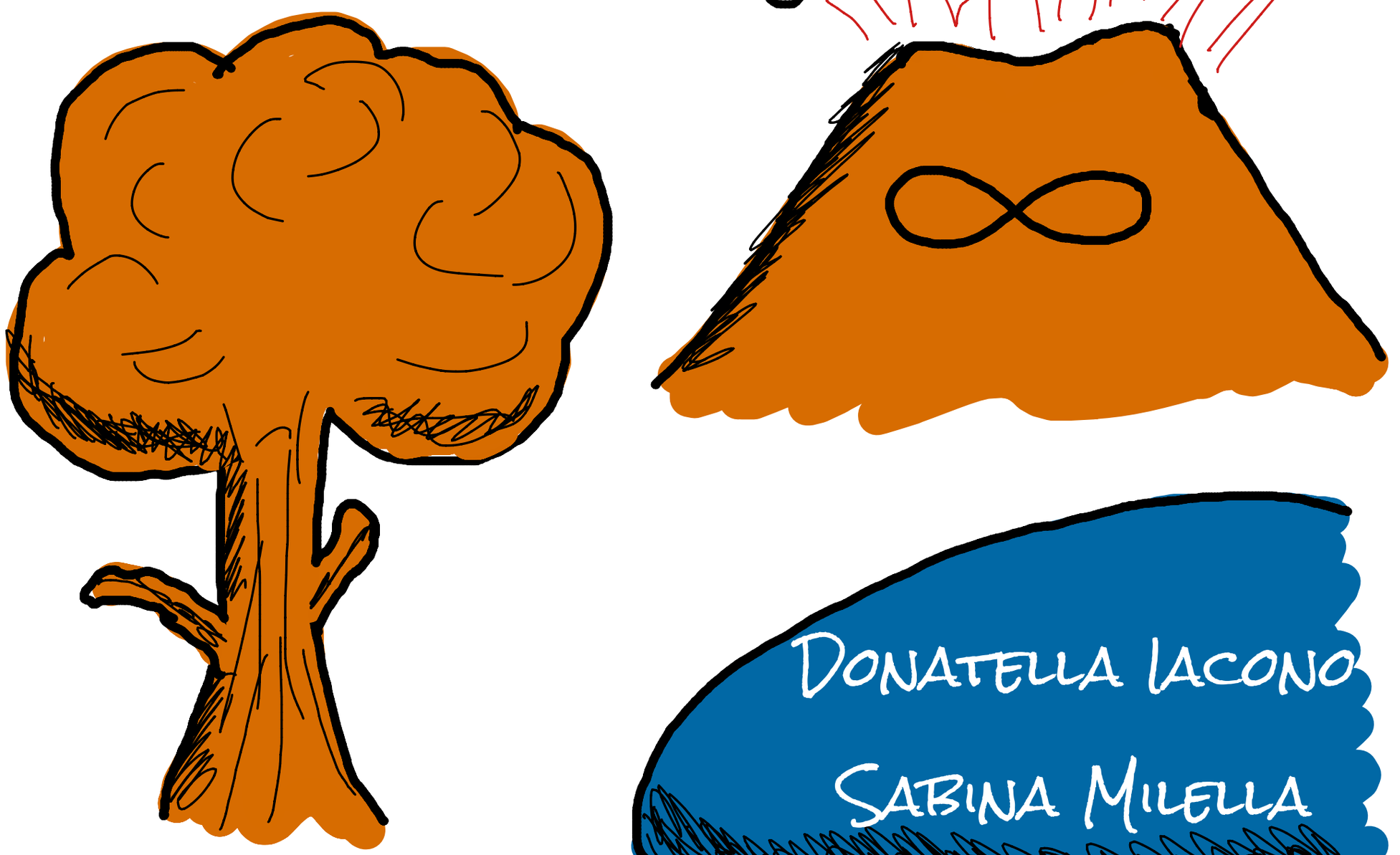
La matematica top secret:

privacy vs big data



Donatella Iacono

Sabina Milella

RSA

iMessage

Skype

privacy

Sky

Whatsapp

Wikileaks

Facebook

MasterCard

Amazon

pgp

Eve

Alice

Bob

Eve

Alice

Bob

Scopo

Spedire un messaggio in modo che solo Bob possa leggerlo e comprenderlo

Come?

modificare il messaggio = cifrare il messaggio

kryptos = nascosto
+
graphia = scrittura

→ crittografia

Eve

Alice

Bob

Scopo

Spedire un messaggio in modo che solo Bob possa leggerlo e comprenderlo

Come?

modificare il messaggio = cifrare il messaggio

Perchè?

- Sicurezza (bancomat, carte di credito,…)
- Autenticazione (firme digitali)
- Privacy (email, chat)
- Pay per view (segnale televisivo criptato)

- Sicurezza (bancomat, carte di credito,…)
- Autenticazione (firme digitali)
- Privacy (email, chat)
- Pay per view (segnale televisivo criptato)

E' un nostro diritto!

Art 15: La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.
La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

Ad ogni lettera si può associare un numero:

- A=0, B=1, C=2…
- A=065, B=066, … (codice ASCII= American Standard Code for Information Interchange)
- basi diverse dalla base 10

……

parola = sequenza di numeri

DA MANIPOLARE!

- Greci e la Scitala

skytale = bastone (400 a.c.)

- Cifrario di Cesare

(chiaro) A B C D E F G H I K L M N O P Q R S T V X

(cifrato) D E F G H I K L M N O P Q R S T V X A B C

MADDMATHS! = PDGGPDALX!

Svantaggi

- non è un sistema sicuro: analisi delle frequenze
- stessa chiave utilizzata per cifrare e decifrare il testo
- come comunicare la chiave?

Svantaggi

- non è un sistema sicuro: analisi delle frequenze
- stessa chiave utilizzata per cifrare e decifrare il testo
- come comunicare la chiave?

Sistema Vernam (1917)

- password lunga almeno quanto il messaggio
- password usata una sola volta : OTP = one time pad
- come scambiare la chiave?

Claude Shannon (1949) ha dimostrato matematicamente che tale sistema è invulnerabile e che tutti i sistemi invulnerabili sono di tipo Vernam.

Su questo sistema si basava la comunicazione sulla linea rossa tra Mosca e Washington durante la guerra fredda.

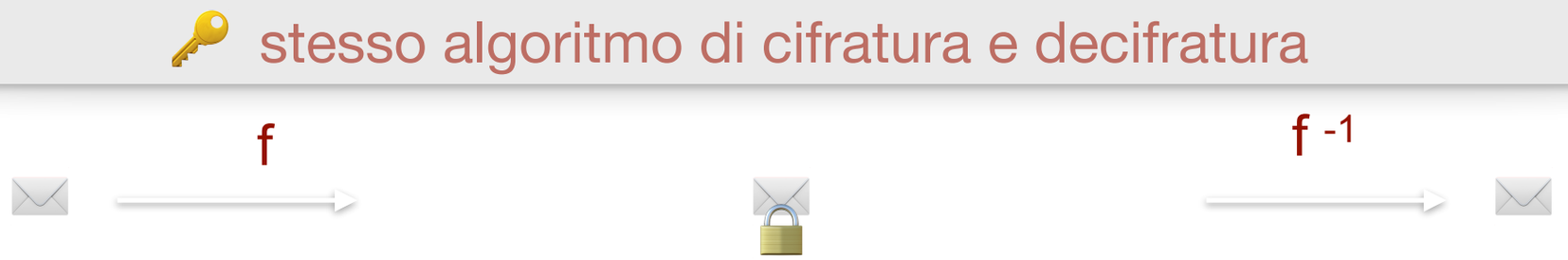
Tutti esempi di Crittografia Simmetrica:

unica chiave usata per cifrare e decifrare

Sistemi crittografici simmetrici più recenti sono

- DES = Data Encryption Standard (inizi anni 70), utilizzato su internet e dalla NSA
- AES = Advanced Encryption Standard (2000)
- IDEA = International Data Encryption Algorithm

🔑 stesso algoritmo di cifratura e decifratura



f serie di operazioni (matematiche) che si possono anche ripetere in maniera inversa.

WIKILEAKS: HTTPS://ARCHIVE.ORG/DETAILS/WIKILEAKSINSURANCE2016

CARNEVALE DELLA MATEMATICA DAL VIVO BY MADDMATHS! DONATELLA & SABINA

wikileaks .org, founded in 2006

“to bring important news and information
to the public”

Guantanamo, Swiss Bank Cayman, Iraq, Afghanistan

Insurance.aes.256 = Assicurazione di Wikileaks

Chiave Privata nei sistemi moderni

- stessi svantaggi dei sistemi classici (possibile vulnerabilità sotto attacchi a forza bruta, scambio della chiave), ma…

- vantaggi: chiavi molto lunghe ed operazioni matematiche difficili da invertire rendono il sistema (teoricamente) inattaccabile per tempi lunghissimi.

- stessi svantaggi dei sistemi classici (possibile vulnerabilità sotto attacchi a forza bruta, scambio della chiave), ma…

- vantaggi: chiavi molto lunghe ed operazioni matematiche difficili da invertire rendono il sistema (teoricamente) inattaccabile per tempi lunghissimi.

👽 Arrivano i matematici!!! 👽

- stessi svantaggi dei sistemi classici (possibile vulnerabilità sotto attacchi a forza bruta, scambio della chiave), ma…

- vantaggi: chiavi molto lunghe ed operazioni matematiche difficili da invertire rendono il sistema (teoricamente) inattaccabile per tempi lunghissimi.

👽 Arrivano i matematici!!! 👽

- fattorizzazione in numeri primi: 2201=31x71

- aritmetica modulare: 2+2=1

Crittografia asimmetrica: ci sono due chiavi, una per cifrare (pubblica) ed una per decifrare (privata).

NON si invia la chiave

- Idea di Diffie ed Helmann (1975)
- Rivest, Shamir ed Adleman (1976): sistema **RSA**

  http://people.csail.mit.edu/rivest/pubs/RSA78.pdf

Crittografia asimmetrica: ci sono due chiavi, una per cifrare (pubblica) ed una per decifrare (privata).

NON si invia la chiave

- Idea di Diffie ed Helmann (1975)
- Rivest, Shamir ed Adleman (1976): sistema **RSA**
  http://people.csail.mit.edu/rivest/pubs/RSA78.pdf

👨 rende visibile la sua chiave pubblica 🔓

👩 invia ✉️🔒

👨 apre ✉️ 🔓 utilizzando 🔑 chiave privata

Crittografia asimmetrica: ci sono due chiavi, una per cifrare (pubblica) ed una per decifrare (privata).

NON si invia la chiave

- Idea di Diffie ed Helmann (1975)
- Rivest, Shamir ed Adleman (1976): sistema **RSA**

La conoscenza della chiave pubblica e dell'algoritmo di cifratura, anch'esso pubblico, non bastano per risalire alla chiave privata in tempi brevi.

Alice sceglie un numero
$n_A = p_A q_A$, p_A e q_A primi molto grandi
ed un numero e_A (chiave pubblica)

n_A e e_A pubblici
p_A e q_A privati

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

Chiave pubblica/privata – sistema RSA 👽

Alice sceglie un numero
$n_A = p_A q_A$, p_A e q_A primi molto grandi
ed un numero e_A (chiave pubblica)

n_A e e_A pubblici
p_A e q_A privati

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

d_A (chiave privata) è tale che $e_A d_A \equiv 1 \pmod{(p_A-1)(q_A-1)}$

Chiave pubblica/privata – sistema RSA 👽

Alice sceglie un numero
$n_A = p_A q_A$, p_A e q_A primi molto grandi
ed un numero e_A (chiave pubblica)

n_A e e_A pubblici
p_A e q_A privati

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

d_A (chiave privata) è tale che $e_A d_A \equiv 1 \pmod{(p_A-1)(q_A-1)}$

Livello di sicurezza?

E' pubblico il numero n_A ottenuto dal prodotto di p_A e q_A e NON i due numeri primi p_A e q_A

La fattorizzazione di un numero molto grande richiede tempi di calcolo molto lunghi.

Chiave pubblica/privata – sistema RSA 👽

Alice sceglie un numero
$n_A = p_A q_A$, p_A e q_A primi molto grandi
ed un numero e_A (chiave pubblica)

n_A e e_A pubblici
p_A e q_A privati

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

d_A (chiave privata) è tale che $e_A d_A \equiv 1 \pmod{(p_A-1)(q_A-1)}$

Bob fa la stessa cosa:
n_B e e_B pubblici
$n_B = p_B q_B$ con p_B e q_B privati

Alice sceglie un numero
$n_A = p_A q_A$, p_A e q_A primi molto grandi
ed un numero e_A (chiave pubblica)

n_A e e_A pubblici
p_A e q_A privati

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

d_A (chiave privata) è tale che $e_A d_A \equiv 1 \pmod{(p_A-1)(q_A-1)}$

Bob fa la stessa cosa:
n_B e e_B pubblici
$n_B = p_B q_B$ con p_B e q_B privati

Alice trasforma il suo messaggio per Bob in un numero M e lo cripta

$$M^{e_B} \equiv C \pmod{n_B}$$

Chiave pubblica/privata – sistema RSA 👽

Alice sceglie un numero
$n_A = p_A q_A$, p_A e q_A primi molto grandi
ed un numero e_A (chiave pubblica)

n_A e e_A pubblici
p_A e q_A privati

e_A non deve avere fattori in comune con $(p_A-1)(q_A-1)$

d_A (chiave privata) è tale che $e_A d_A \equiv 1 \pmod{(p_A-1)(q_A-1)}$

Bob fa la stessa cosa:
n_B e e_B pubblici
$n_B = p_B q_B$ con p_B e q_B privati

Alice trasforma il suo messaggio per Bob in un numero M e lo cripta

$$M^{e_B} \equiv C \pmod{n_B}$$

C è il messaggio cifrato!

😱 da decifrare…

😱 da decifrare…

$$M^{e_B} \equiv C \pmod{n_B}$$

Bob riceve C e lo decifra con la sua chiave privata d_B

$$C^{d_B} \equiv M^{e_B d_B} \equiv M \pmod{n_B}$$

😱 da decifrare…

$$M^{e_B} \equiv C \pmod{n_B}$$

Bob riceve C e lo decifra con la sua chiave privata d_B

$$C^{d_B} \equiv M^{e_B d_B} \equiv M \pmod{n_B}$$

qui si usa che $e_B d_B \equiv 1 \pmod{(p_B-1)(q_B-1)}$

Alice spedisce il messaggio usando e_B (chiave pubblica) di BOB

$$M^{e_B} \equiv C \pmod{n_B}$$

Bob per decifrare usa la sua d_B (chiave privata)

$$C^{d_B} \equiv M^{e_B d_B} \equiv M \pmod{n_B}$$

Chiave pubblica/privata – sistema RSA 👽

Alice spedisce il messaggio usando e_B (chiave pubblica) di BOB

$$M^{e_B} \equiv C \pmod{n_B}$$

Bob per decifrare usa la sua d_B (chiave privata)

$$C^{d_B} \equiv M^{e_B d_B} \equiv M \pmod{n_B}$$

Chiunque può andare un messaggio a BOB fingendosi Alice!

Serve una firma!

- **Firma digitale:** Alice cifra la sua F_A firma con la propria d_A (chiave privata) e lo invia.

$$F_A^{\,d_A} \equiv F \pmod{n_A}$$

- Bob ricevuto il messaggio, lo decifra con e_A (chiave pubblica) di Alice.

$$F^{e_A} \equiv F_A^{\,e_A d_A} \equiv F_A \pmod{n_A}$$

Sicurezza sull'identità di Alice.

- La chiave pubblica di un utente può essere diffusa in diversi modi: in coda ad un messaggio, su server accessibili a tutti…

- Firma digitale: Alice cifra un messaggio con la propria chiave privata e lo invia. Bob, ricevuto il messaggio, lo decifra con la chiave pubblica di Alice.
  Quindi c è sicurezza sull'identità di Alice.

Dalla NSA (National Security Agency) intimarono a Rivest, Shamir ed Adleman di non pubblicare le loro ricerche, loro lo ignorarono e pubblicarono il tutto su un libro del MIT press.

- Zimmermann (1991): PGP = Pretty God Privacy

primo software crittografico pubblico

- tutti possono creare la propria coppia di chiavi (🔒,🔑), pubblica e privata, e rendere nota la chiave pubblica.

- tutti possono criptare ed autenticare i propri file di testo:
  sicurezza email, instant messaging,…

“PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it.”

end to end = da nodo a nodo

- sistema a chiave pubblica/privata
- un software installato sui dispositivi (smartphone, pc,…) di Alice e Bob genera le chiavi
- la chiave privata resta sui singoli dispositivi ed è usata per decifrare
- la chiave pubblica sarà condivisa ed è utilizzata per criptare

il servizio di messaggistica si occupa solo della “spedizione” e non sa leggere i messaggi

end to end = da nodo a nodo

Telegram

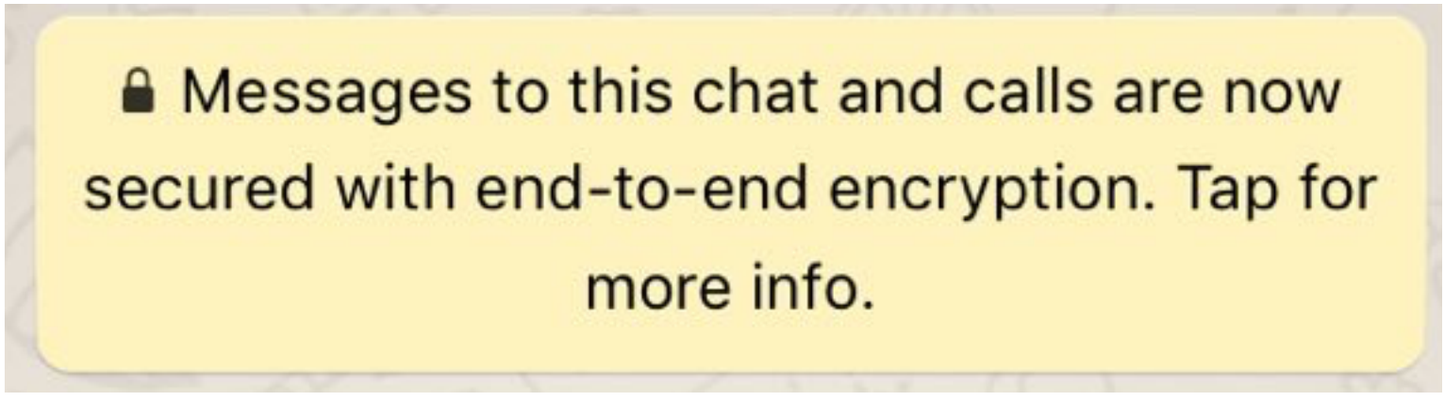
iMessage

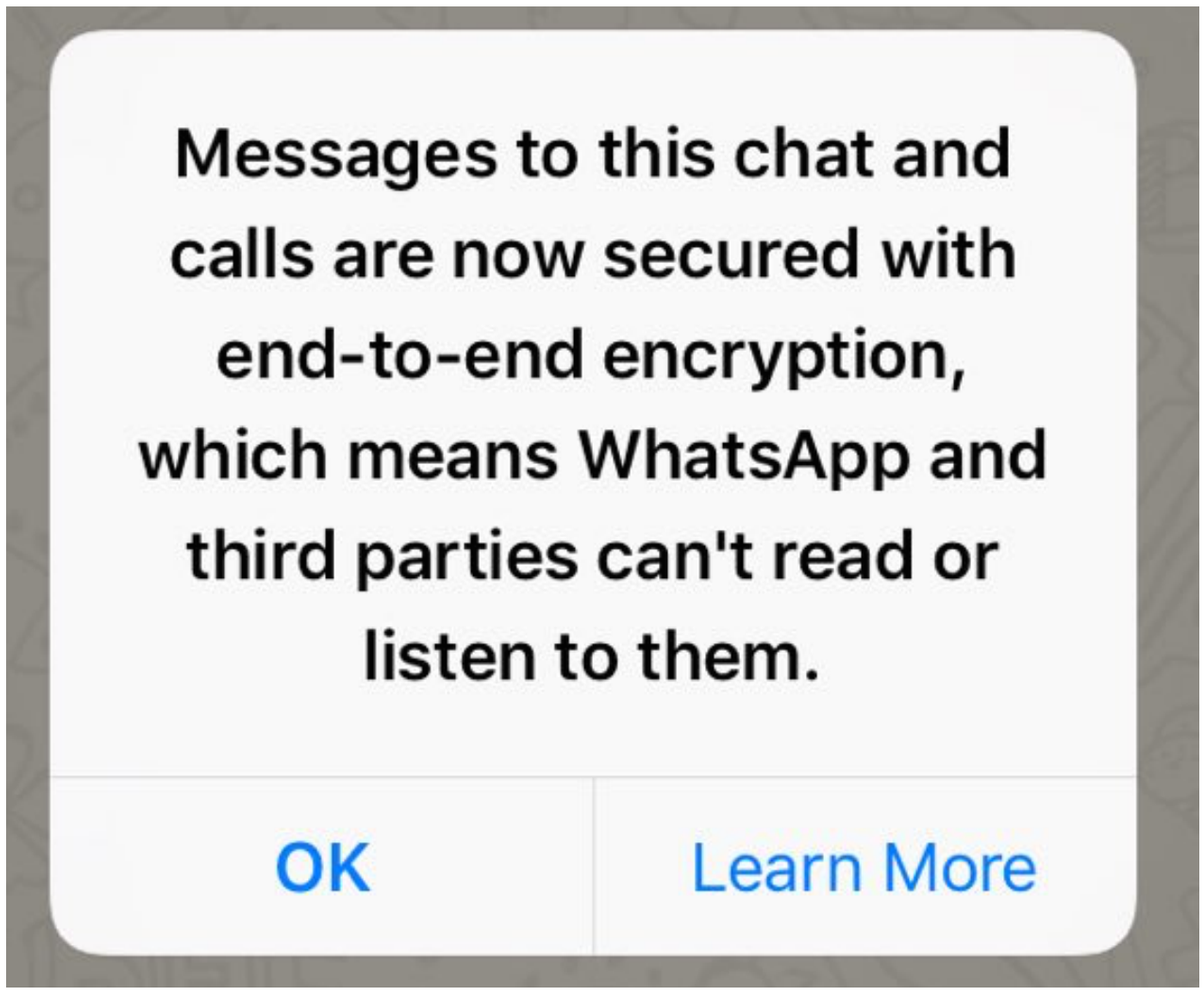
FaceTime

Whatsapp

encryption e decryption **locali**

end to end = da nodo a nodo





https://telegram.org/blog/cryptocontest


BIG DATA

Cosa sono?

Che valore hanno?

Chi li crea?

Come conservarli?

Cosa ci possiamo fare?

Cosa sono? Quantità **enorme** di dati

(Wikipedia)

Termine adoperato per descrivere l'insieme delle tecnologie e delle metodologie di analisi di dati massivi. Il termine indica la capacità di estrapolare, analizzare e mettere in relazione un'enorme mole di dati eterogenei, strutturati e non strutturati, per scoprire i legami tra fenomeni diversi e prevedere quelli futuri.

Insieme di informazioni molto grande (nell'ordine degli Zettabyte) che necessita di metodi analitici ad hoc per le estrazioni di **valore**.

1 megabyte = 10^6 byte
1 gigabyte = 10^9 byte
1 terabyte = 10^{12} byte
1 zettabyte = 10^{21} byte,

Modello delle 3V (Douglas Laney, 2001)

- **Volume:** quantità di dati (strutturati, non strutturati) generati, ogni secondo, da sorgenti di vario tipo.
- **Varietà:** differente tipologia dei dati che vengono generati, collezionati ed utilizzati.
- **Velocità:** velocità con cui i nuovi dati vengono generati e necessità che questi dati arrivino in tempo reale al fine di effettuare analisi su di essi.

In seguito

- **Veridicità:** misura dell'affidabilità.
- **Valore:** capacità di trasformare i dati in valore.

ed ancora altre caratteristiche…

ESEMPI

Dati elaborati quando si utilizza Google

- Ad esempio, quando cerchi un ristorante su Google Maps o guardi un video su YouTube, elaboriamo le informazioni relative a quella attività, che possono includere il video visualizzato, gli ID del dispositivo, gli indirizzi IP, i dati dei cookie e la posizione.

- I tipi di informazioni sopra descritti vengono elaborati anche quando utilizzi app o siti che ricorrono a servizi Google, come gli annunci, Analytics e il video player di YouTube. (Promemoria sulla Privacy di Google)

  Immagini digitali = insieme di pixel —> insieme di numeri (scala di grigio o colore)

Sono incluse informazioni quali i dati sull'utilizzo e le preferenze, messaggi di Gmail, profilo G+, foto, video, cronologia di navigazione, ricerche nelle mappe, documenti o altri contenuti in hosting su Google. I nostri sistemi automatici analizzano queste informazioni quando vengono inviate e ricevute e quando vengono memorizzate.

- Raccogliamo informazioni specifiche del dispositivo (ad esempio il modello del computer o del dispositivo mobile, versione del sistema operativo, identificatori univoci dei dispositivi e informazioni sulla rete mobile, compreso il numero di telefono). Google potrebbe associare gli identificatori del dispositivo o il numero di telefono dell'utente al suo account Google.

Informazioni sui log relativi alle telefonate, ad esempio numero di telefono, numero del chiamante, numeri di deviazione, ora e data delle chiamate, durata delle chiamate, informazioni sull'inoltro di SMS e tipi di chiamate.

Informazioni sulla attività del dispositivo quali arresti anomali, attività di sistema, impostazioni hardware, tipo di browser e lingua, data e ora delle richieste e degli URL di riferimento

Noi e i nostri partner utilizziamo diverse tecnologie per raccogliere e memorizzare informazioni quando viene visitato un servizio di Google, che potrebbero prevedere l'utilizzo di cookie o tecnologie simili per identificare il browser o dispositivo dell'utente. Utilizziamo queste tecnologie anche per raccogliere e memorizzare informazioni quando l'utente interagisce con i servizi che offriamo ai nostri partner, ad esempio servizi pubblicitari o funzioni di Google che potrebbero venire visualizzate su altri siti. Il nostro prodotto Google Analytics consente alle attività commerciali e ai proprietari di siti di analizzare più facilmente il traffico verso i propri siti web e le proprie app. Quando sono utilizzate insieme ai nostri servizi pubblicitari, ad esempio quelli che utilizzano il cookie di DoubleClick, le informazioni di Google Analytics vengono collegate dal cliente di Google Analytics o da Google, utilizzando la tecnologia Google, ai dati relativi alle visite a più siti.

Consentiamo ad aziende di fiducia di utilizzare cookie o tecnologie simili a fini pubblicitari e di ricerca sui nostri servizi. Ad esempio, stipuliamo contratti con aziende che si occupano di valutazioni e utilizzano cookie o tecnologie simili per acquisire informazioni sul pubblico dei nostri servizi, ad esempio i dati demografici degli utenti che visualizzano un video di YouTube o un annuncio. Un altro esempio è rappresentato dai commercianti delle nostre pagine di shopping, che utilizzano i cookie per capire quanti utenti unici visualizzano le schede dei loro prodotti.

https://policies.google.com/privacy

Numerose fonti

- **Human generated:** social networks, portale di e-commerce, siti di recensioni, news…
- **Machine generated:** sensori GPS, IoT, centrali di monitoraggio…
- **Business generated:** pagamenti, ordini, dati di produzione, inventario…

dati.gov.it

Cerca nel sito

Dati Notizie Fare Open Data Federazione dei cataloghi Monitoraggio Sviluppatori Contatti

Elenco Beni Immobili disponibili di proprietà della Città Metropolitana di Napoli

CSV **patrimonio_disponibile.csv**

Grid | Graph | Map | 138 records | « 1 – 100 » | Search data ... | Go » | Filters | Fields

COMUNE	INDIRIZZO	NATURA...	DESTIN...	RENDIT...	TITOLO ...	DATA DI ...	COSTO ...	FITTO	SCHEDA...	LOCAZI...	ATTO DI ...	NOTE/O...	VALORE ...	TE
ARZANO	Via Galil...	BENE PA...	Ex CENT...	1980,00 ...	Atto di v...	-	887000,00	-	-	-	-	-	-	-
FRATTA...	VIA GIUL...	BENE PA...	LOCALE ...	-	ATTO NO...	-	-	-	-	-	-	-	-	-
CAPRI	VIA MARI...	BENE DA...	-	-	-	-	-	attivo	COMUNE...	12000,00	-	-	-	NC
CASAMIC...	VIA MOR...	BENE DA...	CASACA...	-	-	-	-	ATTIVO	locazion...	5460,00	-	Immobil...	242306,00	NC
CASTELL...	VIA VIRGI...	BENE DA...	CASERM...	3461,92	COSTITU...	PRIMA D...	-	ATTIVO	MINISTE...	31607,17	CENSITO...	-	-	NC
ERCOLANO	RAMPE D...	BENE DA...	ABITAZI...	-	ATTO DE...	PRIMA D...	-	LIBERO	-	-	CENSITO...	-	-	NC
ERCOLANO	RAMPE D...	BENE DA...	ABITAZI...	-	ATTO DE...	PRIMA D...	-	ATTIVO	locazion...	5988,00	CENSITO...	-	-	NC
GIUGLIA...	Strada C...	BENE DA...	Tenuta a...	-	ATTO NU...	PRIMA D...	-	ATTIVO	UNIVERS...	10179,04	CENSITO...	Il contrat...	-	NC
Giugliano	Strada C...		Tenuta a...	-	ATTO DE...	PRIMA D...	-	ATTIVO	ASL NAP...	8400,00	-	-	-	-
GIUGLIA...	Strada C...	BENE DA...	Tenuta a...	14496,00	ATTO NU...	PRIMA D...	-	-	Contratt...	8400,00	CENSITO...	L'ARMEN...	-	NC
ISCHIA	VIA MAZ...	BENE DA...	CASERM...	8480,65	COSTITU...	PRIMA D...	-	ATTIVO	MINISTE...	99635,30	DETERMI...	-	-	NC
ISCHIA	PIAZZA D...	BENE DA...	COMMER...	-	CENSITO...	PRIMA D...	-	LIBERO	-	-	CENSITO...	-	206000,00	NC
ISCHIA	PIAZZA D...	BENE DA...	COMMER...	-	CENSITO...	PRIMA D...	-	ATTIVO	locazion...	9949,68	CENSITO...	-	216500,00	NC

www.dati.gov.it

informazioni —> valore

- **Ricerca Scientifica (salute, ambiente, sociale, ….)**
- **Scopi Commerciali (elezioni politiche, pubblicità, …)**

informazioni —> valore

Problemi

- Immagazzinare (server esterni, Cloud)
- **Trasmettere**
- **Manipolare**

in modo sicuro

- Visualizzare
- Analizzare e costruire modelli predittivi

- Immagazzinare (server esterni, Cloud)
- **Trasmettere**
- **Manipolare**

in modo sicuro

- Immagazzinare (server esterni, Cloud)
- **Trasmettere**
- **Manipolare**

in modo sicuro

⚠ La crittografia a chiave pubblica consente un accesso a grana grossa ai dati

—> una unica chiave può decifrare tutto

Alcune soluzioni

- **crittografia funzionale:** chiavi segrete con funzioni specifiche sui dati o su selezioni di dati
- **crittografia omomorfica**

CRITTOGRAFIA OMOMORFICA

Eseguire operazioni sui dati crittografati senza doverli decifrare

- **Idea:** Rivest, Adleman, Dertouzos (1978)
- Il sistema RSA è parzialmente omomorfo (permette solo alcune operazioni sui dati criptati)
- Craig Gentry (2009, tesi di dottorato)—> risolto il problema della crittografia omomorfica totale (brevetto IBM).

Svantaggi

- Non ci sono ancora applicazioni per la crittografia omomorfica totale (IBM?)
- Sistema criticato perché lento, ma giustificato per dati altamente sensibili.

Alcune applicazioni (crittografia omomorfica parziale)

- Microsoft: calcolo statistico del rischio di infarto su dati medici criptati
- MIT (2011): CryptDB

La **DARPA** (Defense Advanced Research Projects Agency), agenzia degli Stati Uniti che sviluppa progetti avanzati per la difesa militare, è interessata alla crittografia omomorfica ed è disposta a spendere 20 milioni di dollari per uno strumento che, manipolando database crittografati, impieghi 100.000 volte il tempo richiesto per lavorare con dati in chiaro.

E come sempre…

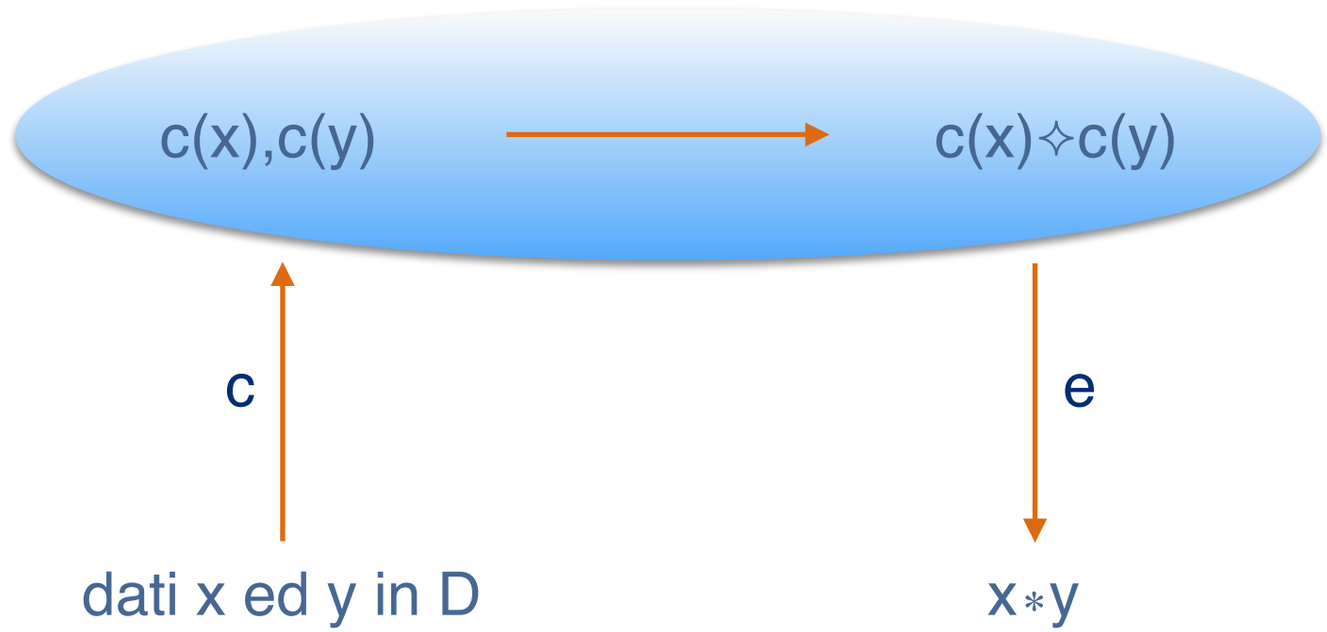
ARRIVANO I MATEMATICI!!!

Omomorfismo: applicazione tra due strutture algebriche dello stesso tipo che conserva le operazioni

Strutture algebriche? 😱
Conserva le operazioni 😱😱

(D,$*$) insieme dei dati in chiaro su cui si vuole effettuare l'operazione $*$
c algoritmo di cifratura
e algoritmo di decifratura
(c(D),$\star$) insieme dei dati in criptati su cui si può effettuare l'operazione $\star$

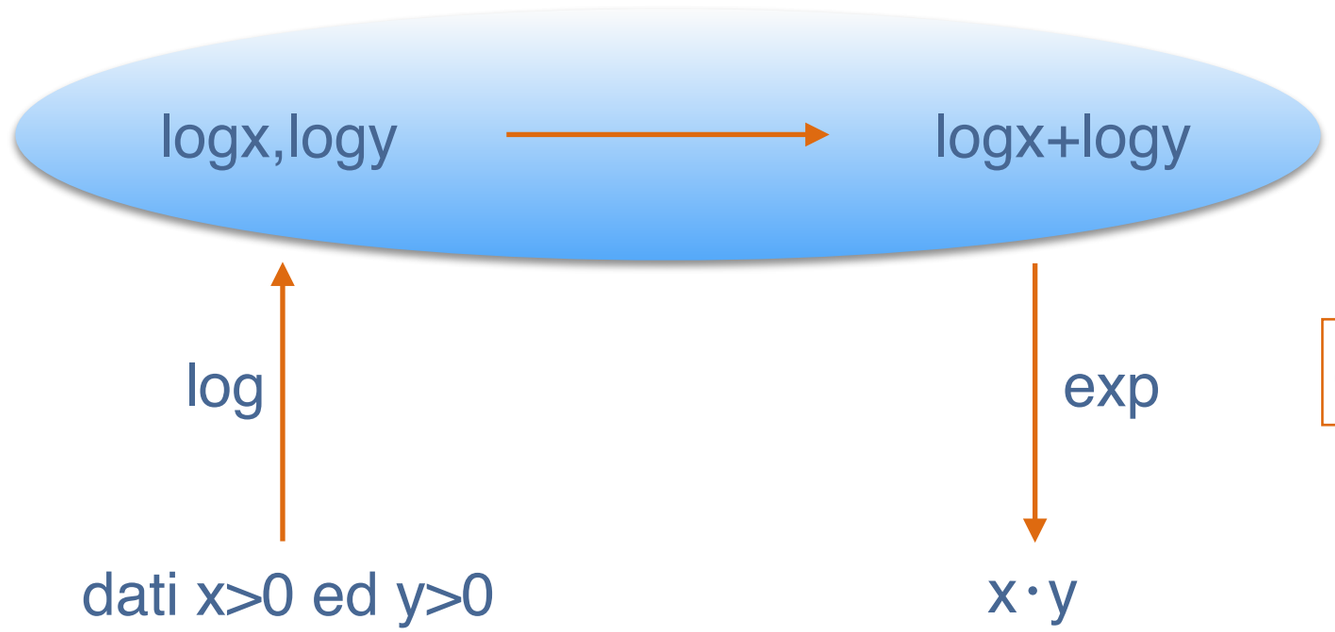
$$c(x*y)=c(x)\star c(y)$$



La funzione c è un omomorfismo tra (D,$*$) e (c(D),$\star$)

$(R_+, \cdot)$ insieme dei dati in chiaro su cui si vuole effettuare l'operazione $\cdot$
log algoritmo di cifratura
exp algoritmo di decifratura
(R,+) insieme dei dati in criptati su cui si può effettuare l'operazione +

$$\log (x \cdot y) = \log x + \log y$$



$e^{\log x + \log y} = e^{\log(x \cdot y)} = x \cdot y$

La funzione log è un omomorfismo tra $(R_+, \cdot)$ e (R,+)

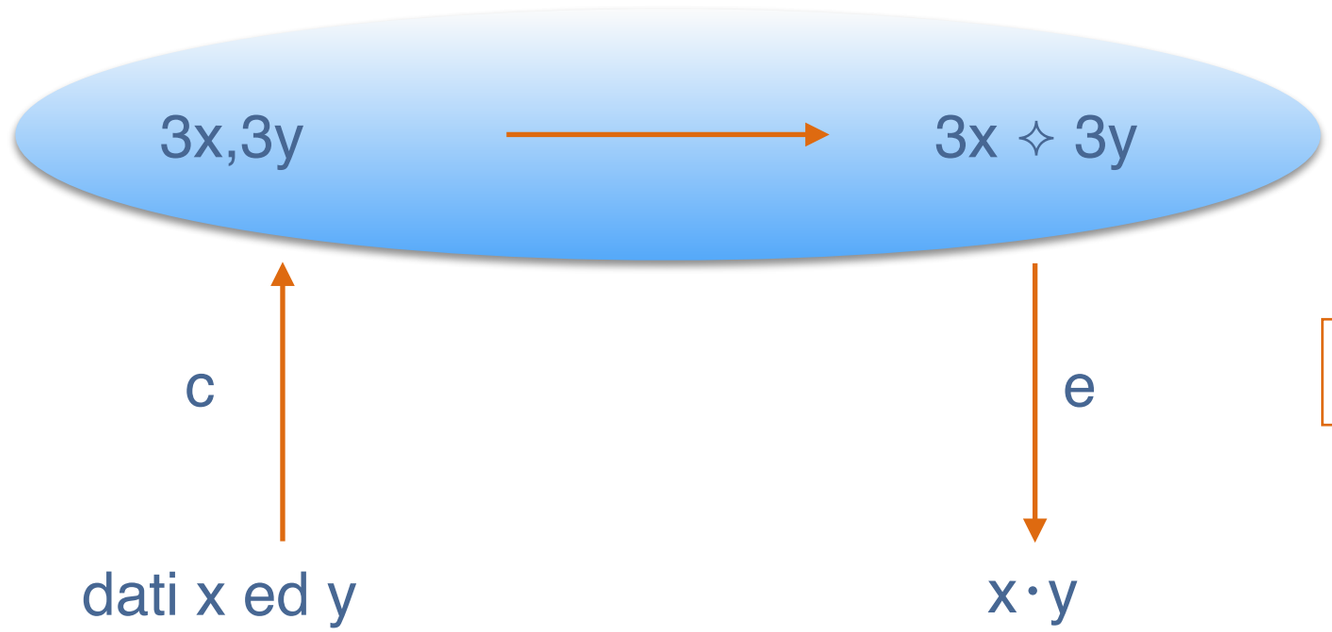
(R,$\cdot$) insieme dei dati in chiaro su cui si vuole effettuare l'operazione $\cdot$

c(x)=3x algoritmo di cifratura

e(x)=x/3 algoritmo di decifratura

(R,$\diamond$) insieme dei dati in criptati su cui si può effettuare l'operazione $\diamond$

$$x \diamond y = (x \cdot y)/3$$



$3x \diamond 3y = (3x \cdot 3y)/3$

La funzione c è un omomorfismo tra (R,$\cdot$) e (R,$\diamond$)

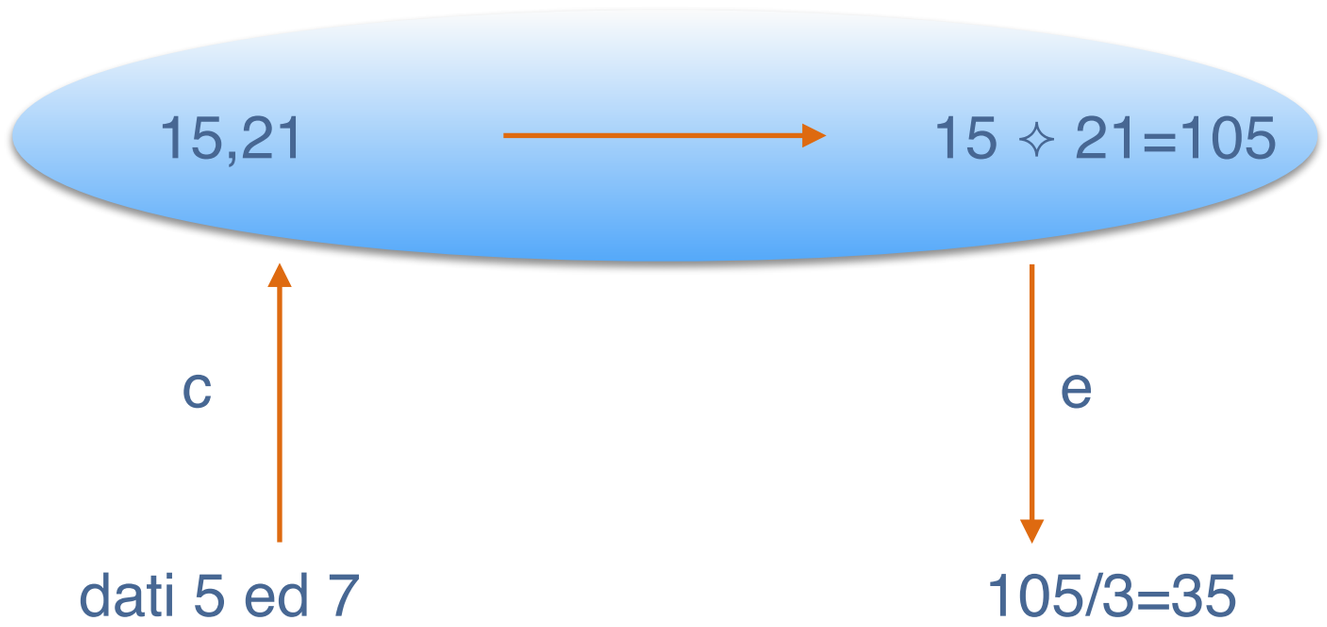
(R,$\cdot$) insieme dei dati in chiaro su cui si vuole effettuare l'operazione $\cdot$

c(x)=3x algoritmo di cifratura

e(x)=x/3 algoritmo di decifratura

(R,$\diamond$) insieme dei dati in criptati su cui si può effettuare l'operazione $\diamond$

$$x \diamond y = (x \cdot y)/3$$



La funzione c è un omomorfismo tra (R,$\cdot$) e (R,$\diamond$)

8Val9XBz80BHb6ul
MxxaIA==

W4zfmOwdV4GueuE9a
Gpagw==

https://www.tools4noobs.com/online_tools/encrypt/

GRAZIE E..

BUON CARNEVALE