Crittografia

Cosa c’è dietro ciò che vede dell’utente?
Quali sono i sistemi per proteggere i dati in rete?

Presentazione della ricerca: “Crittografia”
Di Parisi Matilde

Corso di: Matematica per il Design
ISIA Urbino
A. A. 2023/24

Che cosa succede quando si effettua un login?

Che cos'è il login?

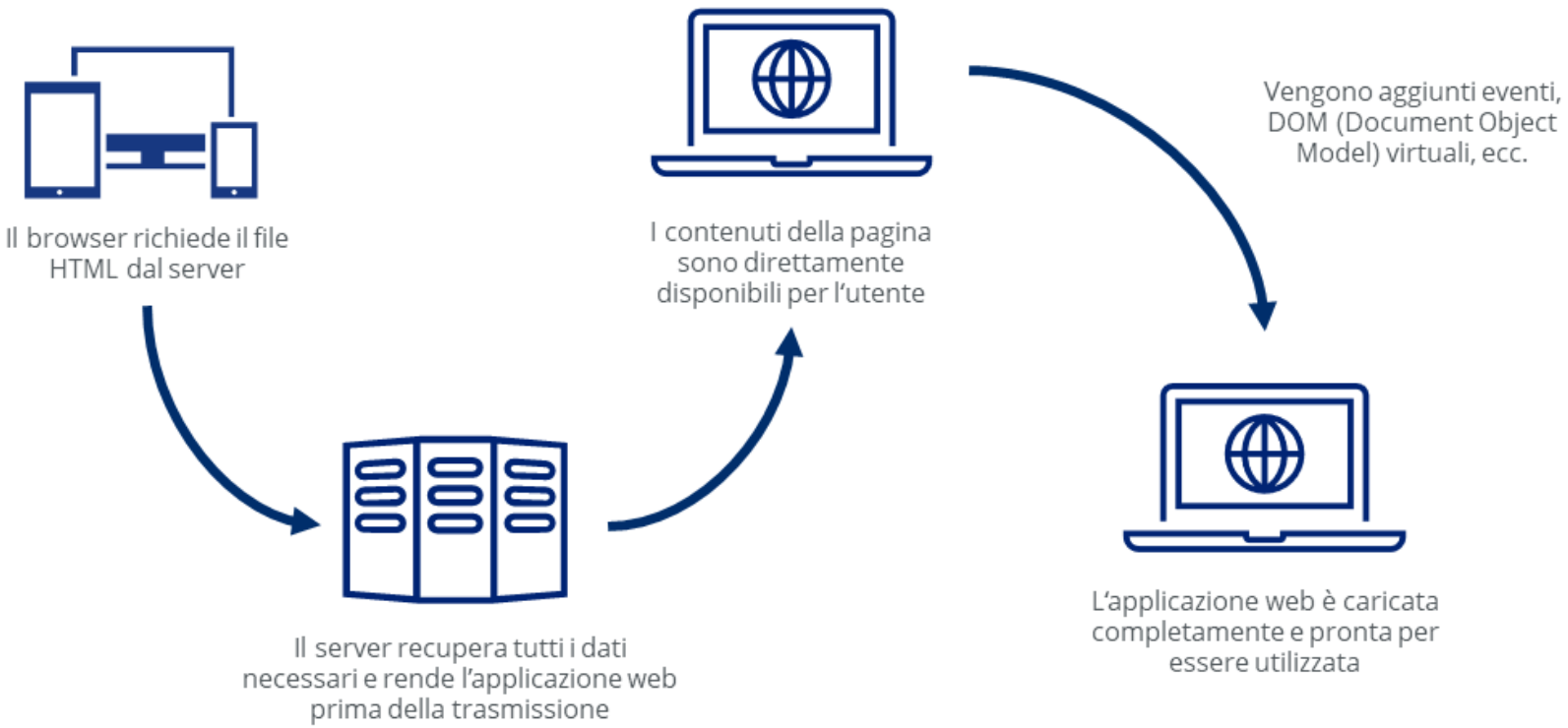
I login è il processo attraverso il quale un utente ottiene l'accesso a un sistema informatico o a un'applicazione. Solitamente coinvolge l'inserimento di credenziali come nome utente e password. Le operazioni di login coinvolgono diversi passaggi, tra cui l'autenticazione dell'utente e l'autorizzazione per accedere alle risorse del sistema.

Modello Client - Server

Dal punto di vista tecnico, operazione che viene svolta è un'interazione tra due componenti:

Client: Un'entità che richiede servizi o risorse dal server.
In un contesto di applicazione web, il client è spesso rappresentato dal browser dell'utente o da un'applicazione mobile o desktop. Il client invia richieste al server e visualizza le risposte ricevute. Può anche gestire l'interazione dell'utente con l'interfaccia grafica e le azioni dell'utente.

Server: Un'entità che fornisce servizi o risorse richieste dai client.
Può essere un server web, un server di database, un server di applicazioni. Il server riceve le richieste dai client, le elabora e restituisce le risposte appropriate.



1. **Richiesta d'accesso**: Il Client (ad esempio, il browser dell'utente) invia una richiesta di accesso al server, fornendo le credenziali dell'utente.

2. **Elaborazione delle credenziali**: Il server riceve la richiesta di accesso e verifica le credenziali dell'utente nel suo database.

3. **Autenticazione dell'Utente**: Se le credenziali sono valide, il server autentica l'utente e crea una sessione di accesso. Questa sessione può essere associata a un identificativo univoco (ad esempio, un token di sessione) che viene inviato al client.

4. **Gestione della Sessione**: Il client riceve l'identificativo della sessione e lo invia al server con ogni richiesta successiva. Il server utilizza l'identificativo della sessione per identificare e gestire l'accesso dell'utente durante la sessione.

5. **Protezione e Terminazione della Sessione**: Il server protegge la sessione di accesso e la termina quando l'utente esegue il logout o quando la sessione scade per inattività.

Che cos’è la crittografia?

La Crittografia (dal greco antico “kryptós”, “nascosto” e “graphía”, “scrittura”) è una disciplina che si occupa di cifrare messaggi e/o testi (creare codici) in modo che non siano più comprensibili, se non tramite l’utilizzo di una chiava di lettura. Questo sistema garantisce la sicurezza del contenuto e l’accesso solo a chi ne è autorizzato.
La crittografia è considerata una branca della “crittologia” e si applica oggi, principalmente a messaggi dal contenuto riservato, ad esempio le conversazioni online tramite le app di messaggistica.

Funzionalità durante il login

Cifrare le credenziali: Le credenziali dell’utente, come nome utente e password, vengono crittografate prima di essere memorizzate nel database del server. Ciò significa che anche se un potenziale intruso riesce ad accedere al database, le credenziali non sono memorizzate in chiaro, rendendo più difficile decifrarle.

Proteggere il token di sessione: Dopo una corretta autenticazione, il server genera un token di sessione (una piccola unità di dati che rappresenta l’autorizzazione per accedere a una risorsa specifica) che identifica univocamente l’utente durante la sessione attiva. Questo token può contenere informazioni sensibili sull’identità dell’utente o sui suoi privilegi di accesso. La crittografia viene utilizzata per garantire che il token di sessione sia protetto durante la trasmissione e non possa essere manomesso o falsificato da terzi.

Protezione delle informazioni sensibili durante la sessione e l’archiviazione sul server, garantendo che siano accessibili solo all’utente autorizzato.

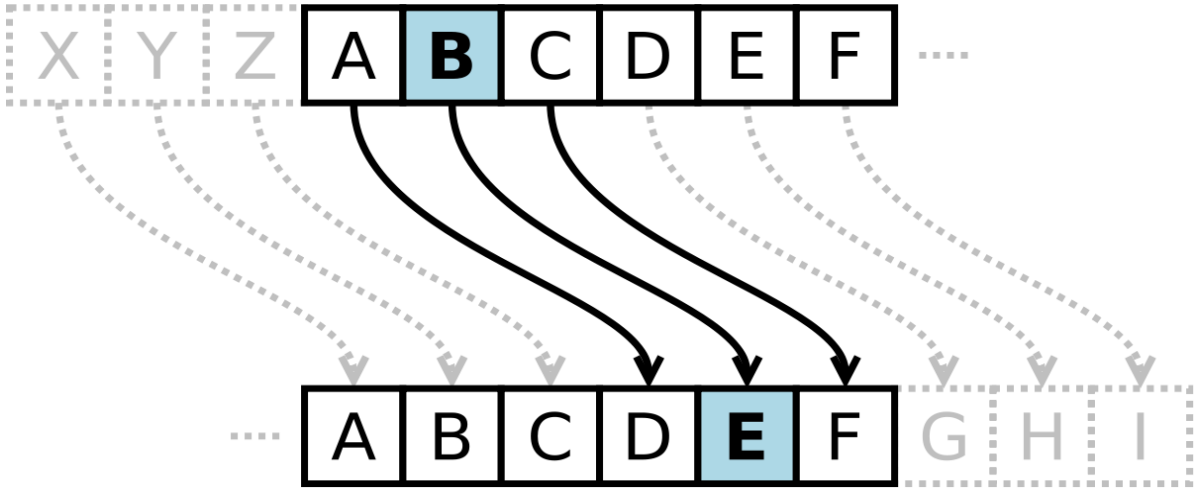
Simulazione cifrario interattivo

https://cryptii.com/pipes/vigenere-cipher

Esempi storici

Cifrario di Cesare (50-60 A.C.)

Il cifrario di Cesare è un cifrario a sostituzione **monoalfabetica**, in cui viene scelta come chiave un numero X da 1 a 26 (totale delle lettere dell'alfabeto); ogni lettera del messaggio in chiaro viene sostituita con la lettera che si trova x posizioni avanti. Questo sistema veniva utilizzato soprattutto per proteggere le comunicazioni private e militari. In particolare, le testimonianze storiche raccontano che Caio Giulio Cesare utilizzasse come chiave di decifratura uno spostamento delle lettere di 3 posizioni.



Cifrario di Vigenère (1586)

Il cifrario di Vigenère è un sistema di cifratura a sostituzione **polialfabetica**, ed anche uno dei più conosciuti. Il metodo si può considerare una generalizzazione del cifrario di Cesare: il sistema sposta le lettere di un numero di posti variabili e l'ammontare della variazione viene deciso in base alle lettere contenute all'interno della chiave, che è detta anche verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte, fino a che abbia lo stesso numero di elementi del testo in chiaro.
Per semplificare la cifratura, Vigenère propose l'uso della "matrice" quadrata, composta da alfabeti ordinati e spostati, che coniugava la "recta tabul"a dell'abate Tritemio, con la parola chiave (contrasegno) proposta da G. B. Bellaso nel suo sistema del 1553.

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

Come funziona la crittografia?

Cifratura

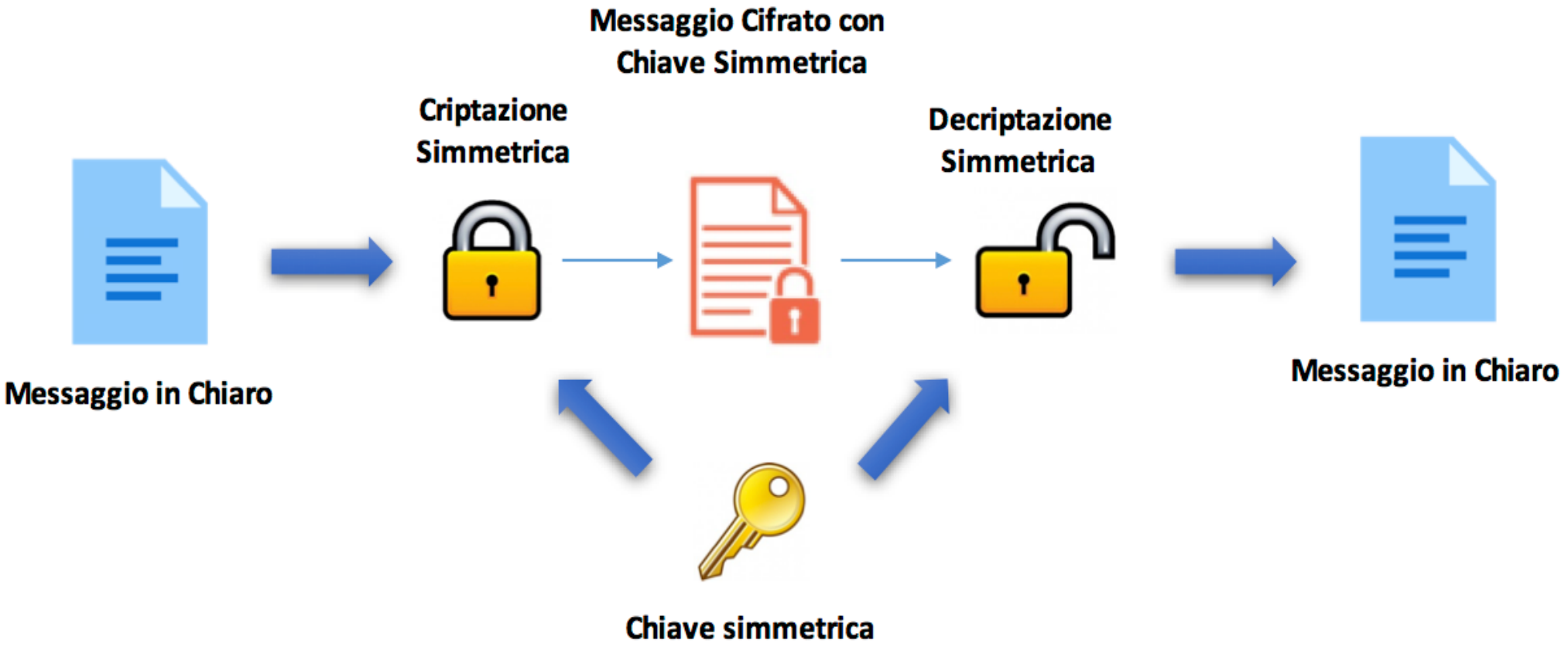
La cifratura è l'applicazione tecnica della crittografia. Le tecniche crittografiche consistono nell'utilizzare un **algoritmo** per codificare il **testo in chiaro** (dati leggibili dagli esseri umani) in **testo cifrato** (un messaggio crittografato). Il messaggio può essere decodificato solo utilizzando una password o una stringa di numeri nota come **chiave di crittografia.** Gli algoritmi avanzati di oggi garantiscono che ogni chiave di crittografia sia casuale e unica, rendendo quasi impossibile che qualcuno la indovini correttamente.
La stessa chiave è quindi necessaria per decifrare i dati e riportarli al loro stato originale. Senza la chiave corretta, anche se si possiede il dato cifrato, è estremamente difficile, se non impossibile, decifrarlo.

Tipologie e funzionalità della cifratura

Ogni algoritmo richiede un certo numero di chiavi, in base al quale viene utilizzato un determinato tipo di cifratura, le principali sono due:

-Cifratura a **chiave Simmetrica**

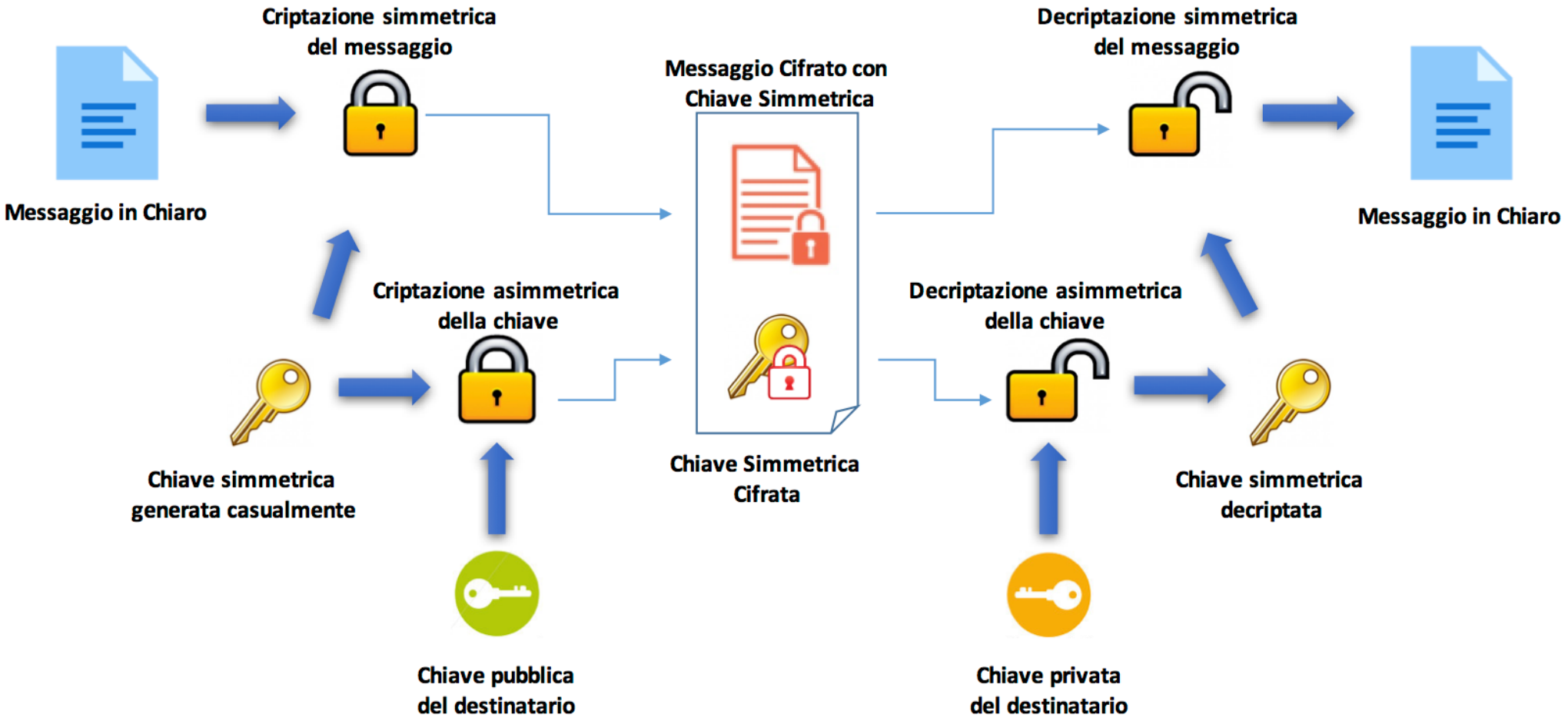
-Cifratura a **chiave Asimmetrica**



La cifratura a chiave simmetrica o (a chiave segreta) è un sistema di decodifica, semplice da implementare e veloce nell'elaborazione. Il processo avviene tramite l'utilizzo di un'unica chiave che serve per codificare e decodificare il messaggio.

PRO
Sistema semplice e veloce grazie alla brevità delle chiavi (128 o 256 bit) che richiedono una modesta potenza di calcolo.

CONTRO
Basso livello di sicurezza, perché l'utilizzo di un'unica chiave presuppone uno scambio di informazione tra le due parti, rischiando che il contenuto venga intercettato.



La cifratura a chiave asimmetrica utilizza due chiavi diverse: la prima chiave è detta " pubblica", viene utilizzata per cifrare il testo e può essere condivisa con chiunque voglia comunicare con il destinatario; la seconda chiave è chiamata "privata", essa serve per decifrare il testo criptato e deve rimanere segreta ad uso esclusivo del destinatario.

PRO
Questo tipo di cifratura garantisce una maggiore sicurezza.
Infatti, riesce a proteggere i dati anche nel caso in cui un utente venga a conoscenza di una delle chiavi di lettura, dato che per accedere alle informazioni avrebbe comunque bisogno anche dell'altra chiave.

CONTRO
Le chiavi sono quindi molto lunghe e complesse, rendendo più sicuro il sistema ma allo stesso tempo rallentando il funzionamento della crittografia nel suo insieme.

Che cos’è un algoritmo?

Algoritmi

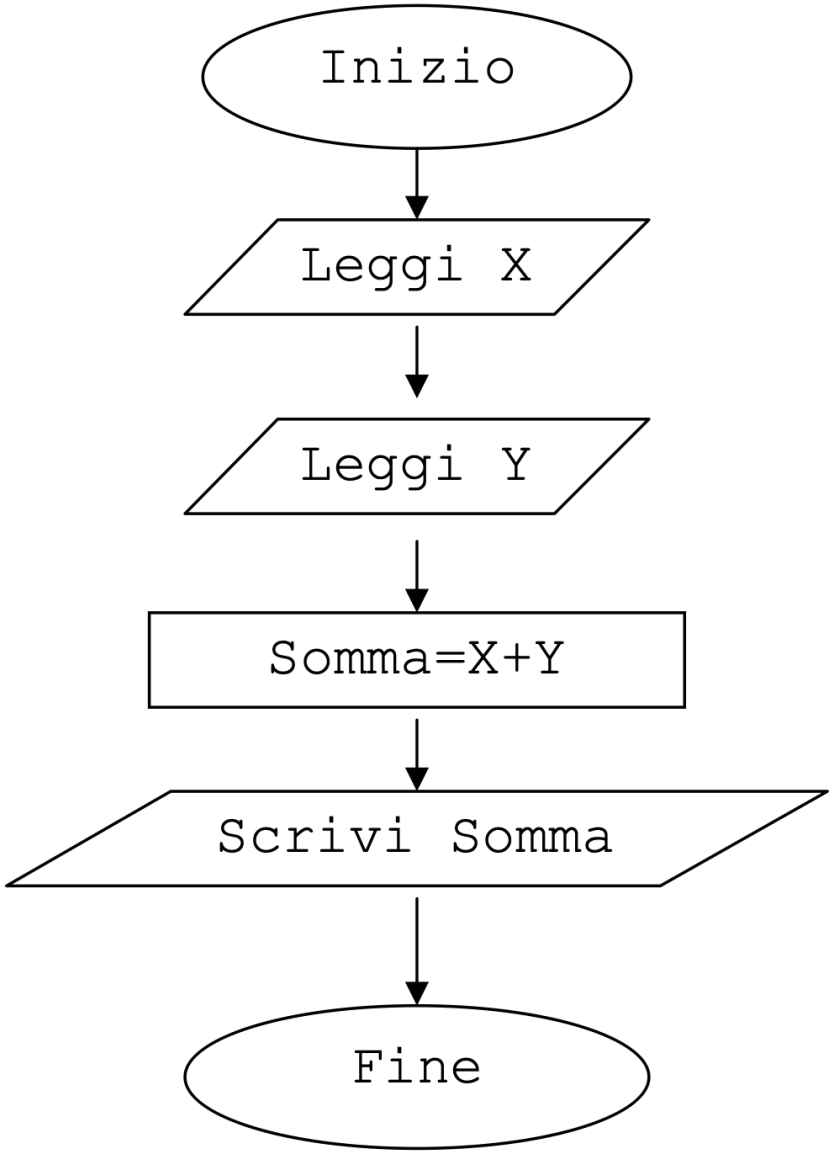
La parola algoritmo deriva dal nome del matematico Arabo Muhammad Al-Khwarizmi, vissuto nell’800 A.C., considerato il padre dell’algebra moderna. L’algoritmo è un qualsiasi processo di calcolo, o meglio una strategia risolutiva di un problema. Affinché questa strategia sia definita algoritmo deve avere delle caratteristiche ben precise:

1.Sequenziale- Deve possedere delle istruzioni elementari che vanno eseguite secondo un ordine ben preciso.
2.Non ambiguo - Deve essere interpretabile in un unico modo.
3.Generale- L’algoritmo deve essere “generale” perché se esso e eseguito da una macchina, questa non sarà in grado di interpretare le istruzioni, ma eseguirà le indicazioni meccanicamente. Lo scopo è essere in grado di risolvere tutta una classe di problemi con la stessa struttura.
4.Eseguibile- Deve essere possibile arrivare alla soluzione.
5.Finito (Terminante)- L’algoritmo deve arrivare ad una conclusione.

L’algoritmo dà luogo ad una computazione effettiva e deterministica, cioè una serie di operazioni che possono essere eseguite e in cui posso determinare le varie soluzioni.
Gli algoritmi come strategie risolutive di problemi possono essere implementati in linguaggi di programmazione (programma), che includeranno l’algoritmo e una sintassi specifica che organizzi le operazioni di input e output delle informazioni.

Rappresentazione dell'algoritmo

Diagramma di flusso

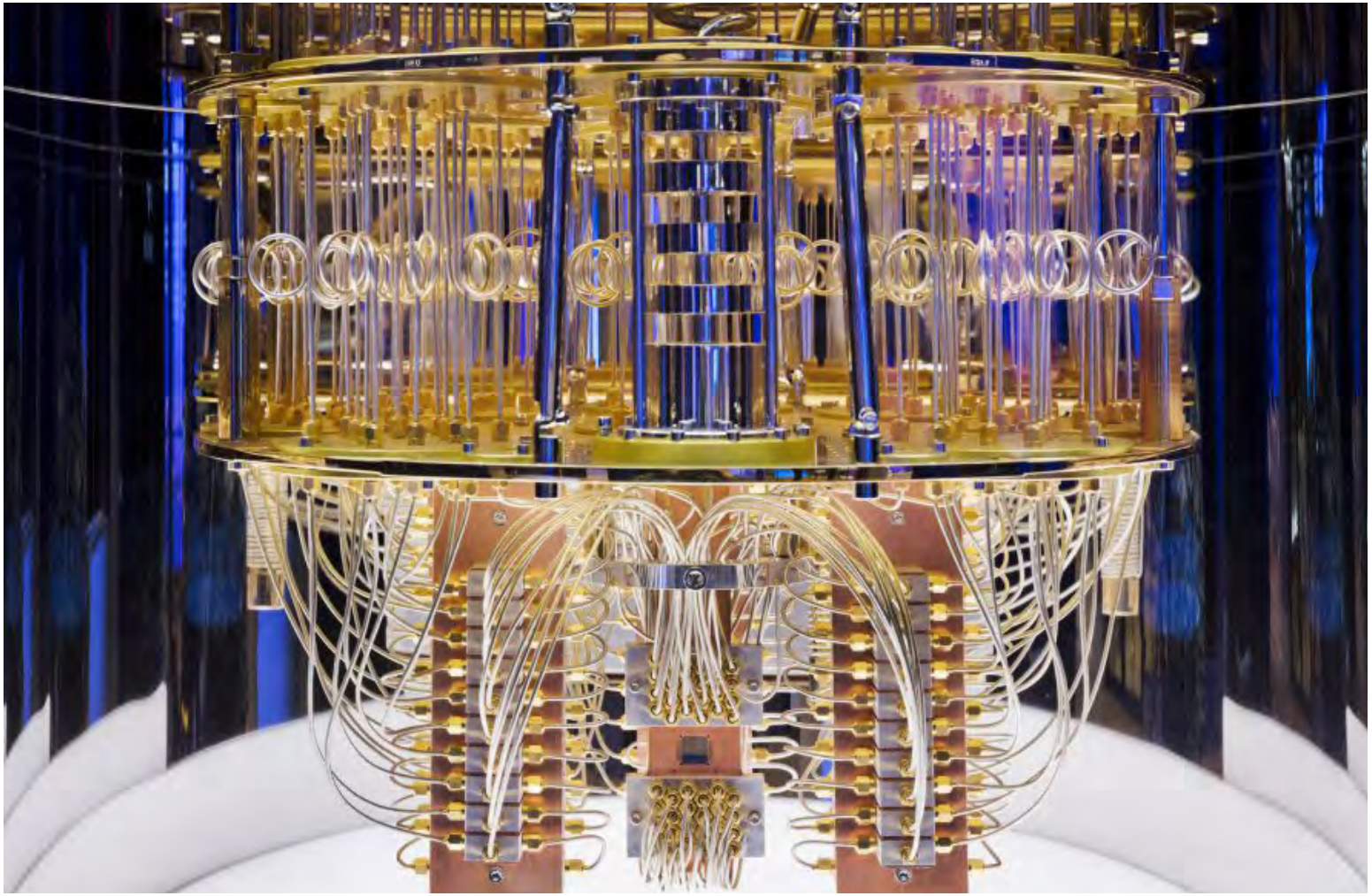


Tipologia di algoritmi

1. **Data Encryption Standard (DES**): uno dei primi metodi di cifratura, è stato sviluppato negli anni ‘70. Il DES è stato a lungo reso obsoleto dall’informatica moderna ed è ormai poco sicuro, di fatto non viene quasi più utilizzato per proteggere informazioni riservate.
2. **Triple Data Encryption (3DES)**: Come suggerisce il nome, 3DES esegue la crittografia DES tre volte cioè utilizza 3 chiavi: ognuna per crittografare, decodificare e ricodificare il messaggio. Sebbene costituisse un’alternativa più forte al protocollo di crittografia originale, da allora è stato considerato troppo debole per i dati sensibili.
3.**Advanced Encryption Standard (AES)**: La crittografia AES è stata il tipo di crittografia più comune sin dalla sua creazione nel 2001. Conosciuta per la sua combinazione di velocità e sicurezza, implementa una tecnica di sostituzione che può avere chiavi da 128, 192 o 256 bit di lunghezza ed è considerato il tipo di algoritmo più sicuro tra quelli attualmente disponibili. AES è lo standard scelto da molti governi, nonché da vari settori privati.
4. **Rivest-Shamir-Adleman** (**RSA)**: Questo sistema asimmetrico prende il nome dai tre scienziati che lo crearono nel 1977. È ancora ampiamente utilizzato oggi ed è particolarmente utile per crittografare le informazioni su Internet con una chiave pubblica o privata.
5.TwoFish: è un algoritmo di cifratura molto rapido, utilizzato in applicazioni hardware e software.
6. **Elliptic Curve Cryptography (ECC**).Essendo una forma avanzata di crittografia asimmetrica, l’ECC si basa sulla scoperta di un logaritmo distinto all’interno di una curva ellittica casuale. Più grande è la curva, maggiore è la sicurezza, poiché ciò significa che le chiavi sono matematicamente più difficili da decifrare. Per questo motivo, la crittografia a curva ellittica è considerata più sicura di RSA.

La crittografia quantistica

Processore fotonico programmabile Borealis della Startup canadese Xanadu.



La crittografia quantistica

Cos'è la crittografia quantistica?

La crittografia quantistica si riferisce a vari metodi di sicurezza informatica per la crittografia e la trasmissione di dati sicuri basati sulle leggi naturali e immutabili della meccanica quantistica. Sebbene sia ancora in fase iniziale, la crittografia quantistica ha il potenziale per essere molto più sicura dei precedenti tipi di algoritmi crittografici e teoricamente è impossibile da hackerare.

Perché è impossibile da hackerare?

Considerando che un atto di spionaggio su un sistema classico può passare infatti inosservato, poiché la fisica classica consente, di effettuare misure senza alterare le proprietà fisiche del sistema, grazie alla crittografia quantistica sarà possibile progettare un canale di trasmissione basato su segnali quantistici, in modo tale che ogni tentativo di spiare il canale causi un'alterazione osservabile del segnale.
La definizione esatta è distribuzione quantistica di chiavi, cioè una trasmissione di dati in grado di vantare una condizione di segretezza perfetta dal punto di vista matematico.

Qual è il rischio per il futuro?

Fino ad oggi, la crittografia dei dati tradizionale è stata generalmente sufficiente per mantenere sicure le comunicazioni nella maggior parte dei contesti di sicurezza informatica. Tutta via, l'aumento del calcolo quantistico pone una minaccia esistenziale anche agli algoritmi crittografici più sicuri. Perché?
Rispetto ai nostri computer classici più veloci e all'avanguardia, i computer quantistici hanno il potenziale per risolvere problemi complessi con ordini di grandezza più rapidi. Significa che quando saranno sviluppati, i computer quantistici saranno in grado di scavalcare in pochi minuti gli attuali protocolli di sicurezza informatica che proteggono i nostri dati.

Come facciamo a proteggerci dai computer quantistici?

Mentre gli informatici di tutto il mondo lavorano giorno e notte per sviluppare una tecnologia quantistica pratica, è fondamentale sviluppare anche nuove forme di crittografia per prepararsi all'era dell'informatica quantistica. Sebbene un tempo i computer quantistici fossero considerati solo teorici, gli esperti stimano che potrebbero mancare solo 20-50 anni per entrare pienamente nell'era dei quanti.

Fonti: Sitografia

https://it.wikipedia.org/wiki/Crittografia

https://www.it-impresa.it/blog/tipi-di-crittografia/

https://www.sealpath.com/it/blog/tipi-di-crittografia-guida/

https://hacktips.it/pillole-crittografia-teorica-1-introduzione-tecniche-classiche-crittografia/

https://www.youtube.com/watch?v=2CcsEPxEz3E

https://www.youtube.com/watch?v=ONHAVGW46D4

https://www.youtube.com/watch?v=FRbZX-mSyz4

https://www.dgroove.it/cose-la-crittografia-e-perche-e-importante-per-la-protezione-dei-dati-in-azienda/4515/

https://www.pandasecurity.com/it/mediacenter/che-cose-la-cifratura-dei-dati/

https://www.treccani.it/enciclopedia/crittografia/#:~:text=Tecnica%20di%20rappresentazione%20di%20un,trasformazioni%20che%20lo%20rendano%20incomprensibile.

https://www.treccani.it/enciclopedia/computer-science_(Enciclopedia-della-Scienza-e-della-Tecnica)/

https://matematica.unibocconi.eu/articoli/enigma

https://www.crocealeramo.edu.it/images/pdf/LA%20STORIA%20della%20crittografia%201%201.pdf

https://cryptii.com/pipes/vigenere-cipher

https://www.devglan.com/online-tools/rsa-encryption-decryption

https://www.entrust.com/it/resources/learn/encryption

https://www.entrust.com/it/resources/learn/post-quantum-cryptography-and-encryption

https://www.ibm.com/it-it/topics/quantum-cryptography#:~:text=Schneider%2C%20Ian%20Smalley-,Cos'è%20la%20crittografia%20quantistica%3F,e%20immutabili%20della%20meccanica%20quantistica.

Fonti: Immagini

Icone:
https://icon-icons.com/it/icona/utente/150670

Modello client server:
https://www.ionos.it/digitalguide/siti-web/programmazione-del-sito-web/script-lato-server-e-lato-client-differenze/

Giulio Cesare:
https://depositphotos.com/it/vector/julius-caesar-100-roman-politician-general-famous-author-latin-prose-216190872.html

Cifrario di cesare:
https://it.wikipedia.org/wiki/Cifrario_di_Cesare

Vigenère:
https://it.wikipedia.org/wiki/Cifrario_di_Vigenère

Cifrario di Vigenère:
https://en.wikipedia.org/wiki/Tabula_recta

Chiave simmetrica/asimmetrica:
https://www.javaboss.it/crittografia-in-java/

Diagramma di flusso:
http://informaticcenter.altervista.org/info3asia15/algsomma.pdf

Computer quantistico:
lickr.com/IBM