La Crittografia

Che cosa si nasconde dietro la trasmissione di dati e come farlo in sicurezza?

Matilde Parisi
Matematica per il Design
A. A. 2023/24

Che cosa succede quando effettuo un login?

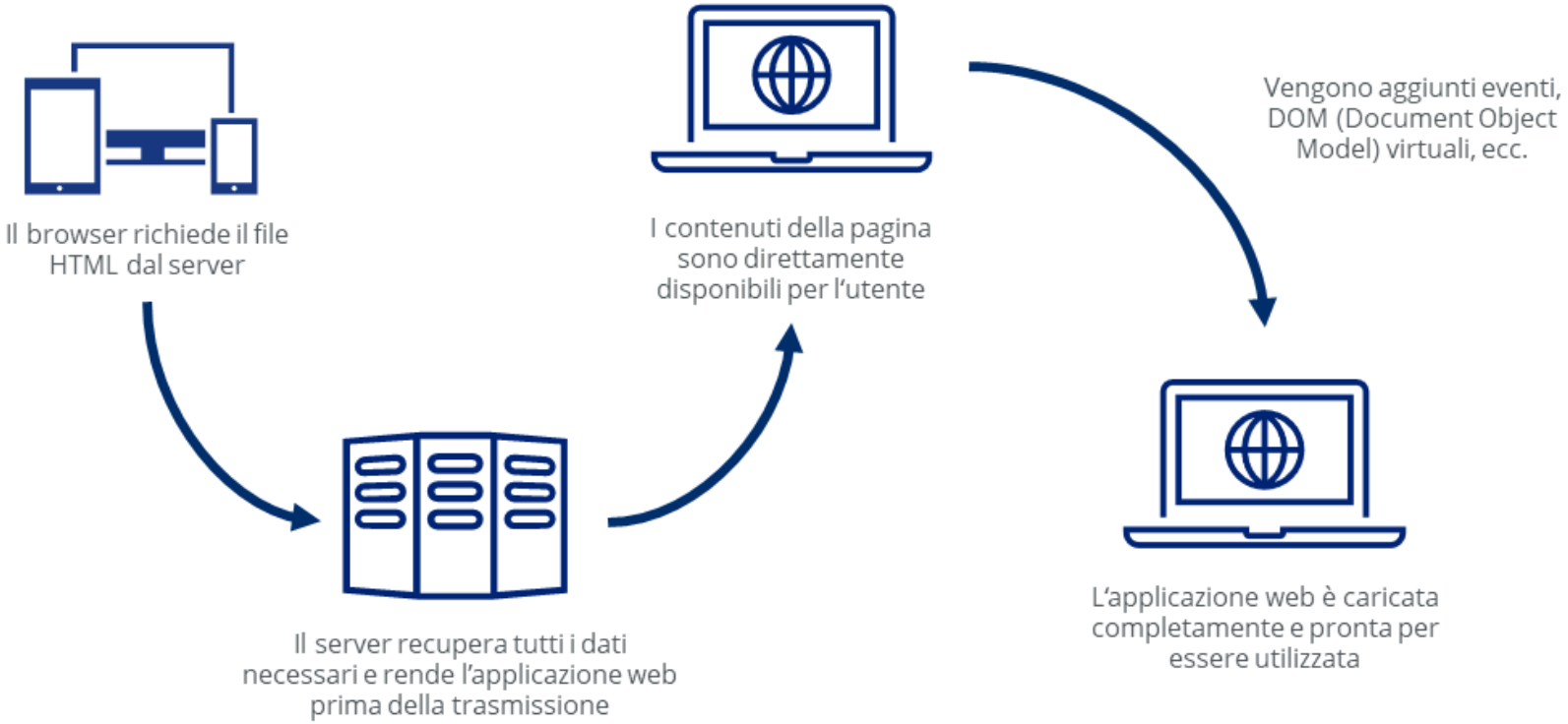
Che cos'è il login?

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.

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.

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 (ad esempio, tramite un cookie) 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.

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.

Come funziona nell’ambito degli accessi online?

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.

Come funziona?

-Cifratura

La cifratura è l'applicazione tecnica della crittografia. Le tecniche crittografiche consistono nel sostituire gli elementi di un messaggio detto "testo in Chiaro" (il testo iniziale da nascondere), mediante gli elementi di un altro sistema di simboli (alfabeto del codice) ottenendo un messaggio cifrato o crittogramma. Per trasformare un messaggio "in chiaro" in un crittogramma, occorre definire delle regole che determinano una classe di trasformazioni.
Per classi di trasformazioni si intende la Chiave Crittografia e gli Algoritmi (di cifratura) che servono ad implementarle.

-Chiave crittografica

La chiave è il codice vero e proprio che utilizziamo per modificare i messaggi, nei moderni sistemi di crittografia, queste chiavi hanno l'aspetto di stringhe di lettere e numeri (codici alfanumerici) che costituiscono il parametro per codificare i messaggi. In genere, la chiave è creata in precedenza e chi crea la chiave dipende dal contesto e dall'applicazione specifica della crittografia. Può essere l'utente che usa il browser, un'autorità centrale, un protocollo di scambio di chiavi o un'entità specializzata.
Una volta stabilita, la chiave viene inserita all'interno dell'algoritmo che decifra il messaggio.

-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.

L'Algoritmo di cifratura utilizza questa chiave per trasformare i dati in un formato cifrato. 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. Ogni algoritmo richiede un certo numero di chiavi, in base al quale viene utilizzato un determinato tipo di cifratura

tipi di algoritmo odierni

Esistono vari tipi di algoritmi di cifratura, ciascuno adatto a determinati scopi e caratteristiche. Ecco i più comuni:

1.Data Encryption Standard (DES): uno dei primi metodi di cifratura, ormai poco sicuro rispetto agli standard odierni e di fatto non viene quasi più utilizzato per proteggere informazioni riservate.
2.Triple DES:con questo metodo, il DES viene applicato 3 volte in modo da rafforzare la sicurezza della cifratura. Utilizza 3 chiavi di 56 bit ed è molto diffuso nell'ambito finanziario.
3.Advanced Encryption Standard (AES): utilizza chiavi da 128, 192 e 256 bit ed è considerato il tipo di algoritmo più sicuro tra quelli attualmente disponibili. AES è lo standard scelto da molti governi e PA, nonché da vari settori privati.
4.RSA: si tratta di un algoritmo di cifratura basato su una chiave pubblica e utilizzato per proteggere i dati condivisi su Internet. Anche se è stato inventato nel 1977, è ancora considerato un metodo efficace, affidabile e diffuso.
5.TwoFish: è un algoritmo di cifratura molto rapido, utilizzato in applicazioni hardware e software.

Tipologie e funzionalità della cifratura

Cifratura a **chiave Simmetrica**

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 per codificare e decodificare il messaggio.

Cifratura a **chiave Asimmetrica**

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.

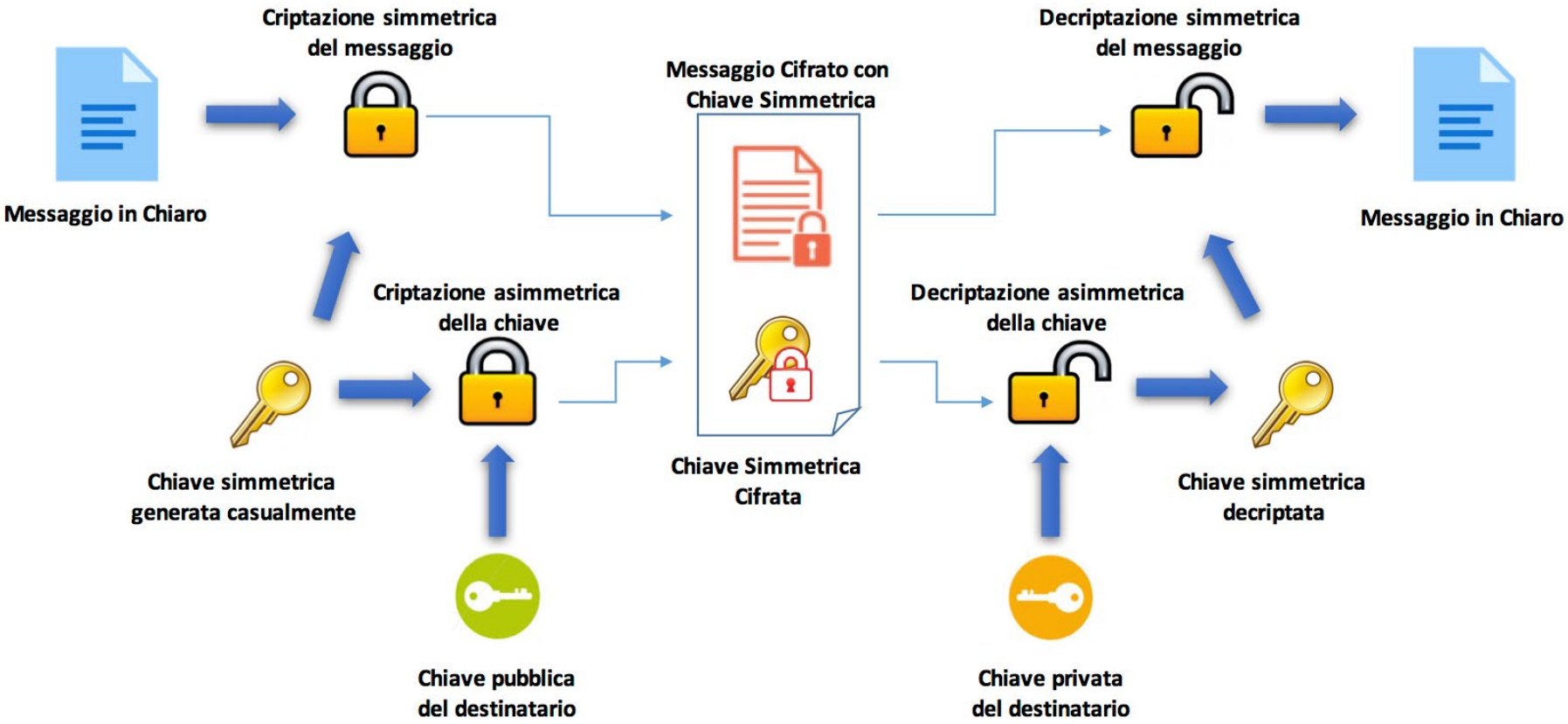
Cifratura a chiave Simmetrica

Schema di funzionamento:
Il testo in chiaro passa attraverso un algoritmo di cifratura, il quale tramite l'utilizzo della chiave, elabora in output il testo cifrato. Il destinatario del messaggio tramite un algoritmo di decifratura, utilizzerà la stessa chiave per ottenere in output il testo decriptato.

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.

Cifratura a chiave Asimmetrica



PRO
Questo tipo di cifratura garantisce una maggiore sicurezza.
Basandosi su due chiavi distinte, 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 due chiavi sono correlate tramite determinati schemi matematiche cioè vengono generate grazie a dei calcoli predefiniti che potrebbero essere sfruttati dagli hacker per forzare la cifratura.
Per ovviare a questa eventualità, 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.

Esempi storici

Crittografia quantistica

La crittografia quantistica è un approccio alla crittografia che, nella fase dello scambio della chiave di decodifica, si serve dei principi della meccanica quantistica. In questo modo si evita che la chiave possa essere intercettata senza che le parti coinvolte se ne accorgano. Entrando nel dettaglio, 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. L'obiettivo è infatti creare una sorta di cifrario perfetto che non prevede un momento di scambio su un canale necessariamente sicuro.

Vantaggi e svantaggi

È importante precisare che la crittografia quantistica è sì una tecnologia ancora in via di sviluppo, ma che può già essere applicata – nonostante le limitazioni – portando dei sostanziali vantaggi.

Con questo tipo di cifratura, infatti, si prevede di rivoluzionare radicalmente il modo in cui le informazioni verranno comunicate, sfruttando le leggi della fisica piuttosto che gli attuali algoritmi matematici. Questa tecnica promette quindi di essere impenetrabile e dovrebbe distribuire le informazioni garantendo un livello di sicurezza senza pari, codificandole su stati quantistici della luce.

Gli strumenti e i dispositivi utilizzati, inoltre, sono in costante miglioramento ed evoluzione e ci si aspetta che in futuro questa tecnologia diventi di uso comune in molte realtà.

Lo svantaggio è che la crittografia quantistica, oggi, è ancora una tecnica nuova e richiede infrastrutture particolari e costose da costruire.

Inoltre le distanze su cui è stata eseguita e testata sono ancora limitate con tassi di errore significativi.

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

http://wwwusers.di.uniroma1.it/~reti/Reti_Elab_html/Cap8.pdf