Crittografia
Scrivere una relazione minimo due pagine massimo cinque pagine :

Non dimentichiamoci che chiunque può accedere alla rete anche chi non ha buone intenzioni e che le applicazioni sono infatti sono sempre più vulnerabili (basti pensare a quelle bancarie e fiscali)Per questo motivo da qualche tempo si sta adottando il protocollo HTTPS che al tradizionale HTTP (con cui i dati viaggiano dati sempre in charo)aggiunge algoritmo crittografico LTSe di un certificato digitale utile a dichiarare l'identità del server remoto e del soggetto che lo gestisce.

QUANDO SI PARLA DI ALGORITMO CRITTOGRAFICO FONDAMENTALMENTE OFFRA:

1. **autenticazione** processo che permette di attestare l'identità di ciascun partecipante ad una comunicazione;
2. **segretezza** indispensabile fare in modo che nessuno possa leggere un messaggio fatta eccezione per il destinatario;
3. **integrità** la protezione da modifiche nonautorizzate operate sul messaggio trasmesso(il materiale inviato al destinatarionon deve oter essere alterato prima della consegna);
4. **non ripudio** un meccanismo atto a fornire le certezze che chi trasmette un messaggio non possa negare di averlo inviato.

Questi elementi fanno si che il cybercriminale non compia attachi come quello dello sniffing o spoofing il primo permette di spiare il contenute dei pacchetti dati trasmessi alla ricerca di informazioni utili,il secondo è mirato agli indirizzi IP,si concentra a quello realmente usato dall'agressore.

La crittografia è la tecnica di un messaggio in forma tale che l'informazione in esso contenuta possa essere recepita solo dal destinatario ciò si può ottenere con due diversi metodi celano l'esistenza stessa del messaggio o sottoponendo il resto del messaggio a trasformazioni che lo rendono incomprensibile.crittografia ha trovato larga applicazione fino dal tempo dell'impero Romano con Giulio Cesare fino hai tempi nostri nella sottile arte militare,diplomatica commerciale e il suo sviluppo è stato fortemente condizionato dall'evoluzione delle tecnologie di comunicazione adottate in questi campi.

Le tecniche sono scrittura invisibile ottenta mediante inchiostro invisibile ottenuta mediante l'utilizzo di inchiostri simpatici ovvero sostanze che una volta asciugate risultino invisibili finche non sono sottoposte all'esposizione di un determinato reagente come il succo di limone per i pirati o la cosi definita copia con carboncino,

Per la comprensione dello stesso messaggio è stata svilupata una tecnica molto valida a partire dal secondo conflitto mondiale Enigma che comprendeva una dissimulazione dell'informazione,ottenuta nascondendo il messaggio in un testo il cui significato sia appartemente estraneo all'informazione del trasmittente.

Le tecniche di crittografia consistono nel rappresentare gli elementi di un messaggio,mediante gli elementi di un altro sistema di simboli,alfabeto del codice ottenendo un messaggio in codice o crittogramma. Per la trasformazione del codice crittogramma occorre definire delle regole che determinano una classe di trasformazioni.Quella veramente adottata viene individuata dal valore assunto da un parametro detto chave sulla cui segretezza si basa la sicurezza del sistema crittografico,un codice è un sistema in cui gli elementi del testo in chiaro sono parole o frasi che vengono sostituite da gruppi di lettere o di cifre che generalmente lunghezza fissa,mentre un cifrarioè un sistema in cui gli elementi del testo in chiaro sono singoli caratteri.

La crittografia è un dogma dove si vuole intendere e volere racchiudere la protezione degli stessi dati. Molti utenti però ancora oggi,continuano a scambiarsi costantemente informazioni senza sentire il bisogno di proteggere i propri dati sensibili e rischiando a renderli accessibili a chiunque.questo perchè manca ancora la cultura e la formazione su queste tematiche di sicurezza.

Che cos'è dunque la crittografia?

Si tratta della conversione dei dati da un formato leggibile in un formato codificato che può essere letto o elaborato solo dopo che è stato decrittato. Solo la persona autorizzata può decriptare i dati e accedere alle informazioni nel formato originale. Ci sono un sacco di metodi per criptare e decriptare i dati, ma la chiave del successo non sta nell'algoritmo. La cosa più importante è mantenere segreta la chiave crittografica (password), o meglio fare in modo che la conoscano solo le persone autorizzate.

La crittografia è la base della protezione dei dati ed è il modo più semplice e importante per garantire che le informazioni di un sistema informatico non possano essere rubate e lette da qualcuno che voglia utilizzarle per scopi malevoli.

Impiegata sia dai singoli utenti che dalle aziende di qualsiasi dimensione, è ampiamente utilizzata su Internet per tutelare le informazioni utente inviate fra il browser e il server e proteggere i dati sensibili dei loro server e database.

Oggi la comunicazione – di qualsiasi genere – ha acquisito un ruolo sempre più centrale nella vita di ognuno di noi; nell'era di internet miliardi di informazioni (anche sensibili) sono in circolazione sulla rete. Per questi motivi si è reso ancor più necessario lo sviluppo di sofisticati sistemi capaci di garantire un elevato livello di confidenzialità di alcuni di questi dati.

La cifratura informatica come la conosciamo oggi, è una materia in costante evoluzione. E proprio per questo suo continuo evolversi, gli esperti consigliano di non affidarsi mai all'ultimo algoritmo crittografico uscito: paradossalmente, infatti, una maggiore sicurezza viene garantita da sistemi già conosciuti e quindi testati pubblicamente (caratteristica che non può ovviamente essere garantita nel caso degli algoritmi più nuovi). Non solo: gli esperti del settore raccomandano anche di attenersi e affidarsi solo alle notizie ufficiali, come quelle rilasciate dal National Institute of Standards and Technology.

La crittografia, dunque, può essere definita un sistema che tramite l'utilizzo di un algoritmo matematico agisce su una sequenza di caratteri, trasformandola. Tale trasformazione si basa sul valore di una chiave segreta, ovvero il parametro dell'algoritmo di cifratura/decifratura. Proprio la segretezza di questa chiave rappresenta il sigillo di sicurezza di ogni sistema crittografico (a questo proposito è interessante la distinzione tra encoding (codifica) e encryption (crittografia), dove la prima serve a facilitare l'immagazzinamento o la trasmissione dei dati, la seconda a mantenere l'informazione segreta).

Al di là dell'ovvio vantaggio di proteggere le informazioni private da furti e violazioni, la crittografia è anche un mezzo per dimostrare che le informazioni sono autentiche e provengono dall'origine dichiarata. Può essere utilizzata per verificare l'origine di un messaggio e confermare che non è stato alterato durante la trasmissione.

Tipi di cifratura

Sulla base della chiave utilizzata, possono essere individuati due tipi di cifratura:

•a chiave simmetrica, noto anche come algoritmo a chiave segreta, dove i messaggi sono decodificabili solo dalla persona che conosce la password. Questi schemi crittografici non vengono di norma utilizzati sulla rete Internet perché la password non può ovviamente viaggiare sullo stesso canale (altrimenti potrebbe diventare preda di utenti malintenzionati interessati alla decodifica del messaggio). La password può essere al limite condivisa usando altri canali ma non è certo l'approccio migliore per scambiarsi messaggi con utenti remoti.

•a chiave asimmetrica: questo metodo utilizza due chiavi diverse, pubblica (che può essere condivisa con chiunque) e privata (che deve rimanere segreta).

Per cifrare un testo, quindi, con la crittografia asimmetrica basta usare la chiave pubblica del destinatario del messaggio mentre quest'ultimo per la decodifica dovrà essere necessariamente in

possesso della sua chiave privata.
Infine, esiste un terzo tipo di crittografia, cosiddetta end-to-end(usata principalmente da WhatsApp, Messenger o Telegram), che permette di proteggere la privacy e le comunicazioni usando doppio paio di chiavi crittografiche necessarie per cifrare e decifrare i messaggi in viaggio da un capo all'altro della comunicazione. Ogni utente, infatti, utilizzerà una chiave pubblica e una chiave privata, legate tra loro in maniera indissolubile. La chiave privata è destinata a rimanere sul dispositivo dei due "comunicanti" e servirà a decrittare i messaggi in arrivo; la chiave pubblica, invece, sarà condivisa con l'interlocutore e sarà utilizzata per crittografare i messaggi in uscita. Questa cifratura permette di rendere innocui tentativi di attacco man in the middle, che puntano proprio a rubare dati e informazioni personali "intercettando" le comunicazioni tra due o più utenti.
Conclusioni
La crittografia, nell'ambito della sicurezza informatica è diventata pertanto (anche grazie all'introduzione del GDPR – General Data Protection Regulation) uno strumento fondamentale per proteggere i dati, archiviati o in transito, da accessi non autorizzati o occhi indiscreti, ma soprattutto è diventata necessaria da divulgazioni accidentali che potrebbero avvenire per inconsapevolezza degli utenti che trattano le informazioni non nel modo corretto, permettendo di conseguenza furti dei dati o altri eventi infausti.In azienda, oltre all'introduzione del protocollo HTTPS, questo sistema di cifratura è stato implementato anche a livello dei file sugli archivi aziendali per lo scambio dei messaggi all'interno dell'universo aziendale, quali ad esempio firma digitale dei messaggi e-mail inviati o chat cifrate.
Solo il comprendere ed implementare in modo corretto i singoli passaggi, come quelli segnalati, mette l'azienda e i suoi preziosissimi asset produttivi (che tipicamente corrispondono a dati archiviati e gestiti) al riparo da buona parte dei rischi informatici in modo semplice da implementare e sicuro da buona parte degli attacchi informatici.