Parlante 1 00:00:00
E molti di qui seguiva questo mondo, aveva già seguito, come dire, sicurezza, la triennale. E quindi magari io davo per scontato in maniera molto errata, e sapevate cos'era la crittografia?
Poi veniva dall'esame e uscivano le varie le accezioni fantastiche e bisogna un attimo.
Di gustare.
Che cos'è la crittografia? Altrimenti non lo segue. Sicurezza dei dati, salvo delle aperture a distinguere un cifrario blocchi da un flusso.
Bibliografia cinetica cinetica, quindi ovviamente non andiamo molto nei dettagli matematici, questo è un posto che il collega proprio su questi argomenti, però per chi non segue se tutti del percorso sicurezza.
No e quindi faccio bene se non seguite l'evento di crittografia.
No, e allora faccio bene a fare questo?
Parlante 2 00:00:58
Non voglio dire ripasso perché.
Parlante 1 00:01:00
Anche perché quando poi parleremo dal blockchain, parleremo dell'hashing.
Quando parleremo della parte normativa del consulente prudenziale parleremo della bibliografia. Un trattamento, quindi uno dei capelli. Di cosa stiamo parlando?
Produciamo un po' di contesti di base, anche con una definizione che ci siamo già ritrovati, della sicurezza, essere.
Come dire, la garanzia di per proprietà.
Integrità, disponibilità, questo ci siamo, no?
Ogni proprietà richiede delle degli strumenti di protezione.
Parlante 2 00:01:38
Fondamentalmente sono delle misure tecnico organizzative e normative per coprire queste proprietà e ovviamente io vado a garantire queste proprietà perché mi trovo in un contesto insicuro o avversario in cui queste proprietà ci sono minacciate da pochi articolari comportamenti i principali contesti di di insicurezza avvengono o nell'ambiente della memorizzato dei dati. I dati sono memorizzati?
Computer, un database con un file e ovviamente il di possono essere vulnerabili.
Ad esempio il database può essere acceduto da chi non dovrebbe farlo. Mi rubano il dispositivo e tutti i file di questo contenuto sono vulnerabili. Sono alla Mercedes il dispositivo ovviamente un'altro contesto di insicurezza e fanno i dati vengono trasferiti.
Se io invio il dato a lui, ovviamente esce dal mio contesto di sicurezza e entra nel suo, ma facendolo deve attraversare parecchio rete che per sua natura è insicura.
O vulnerabile.
Perché in realtà le reti non sono state progettate per essere mesi sicuri?
Il video.
Parlante 1 00:02:52
In futuro?
Sì, sì.
Parlante 2 00:02:58
Tipico errore che facevate ancora di carburatore è dire this in qui è un protocollo sicuro.
E di un po' di meno l'IVA per te?
3000 volte detto ICP affidabile non è sicuro.

Quindi ovviamente può può avere i messaggi vostra essere intercettati, i dispositivi che costituiscono la rete possono comportarsi in maniera non propriamente corretta e quindi una maniera Rete Unite oppure il protocollo stesso protocollo di sicuro.
Ovviamente se io voglio andare a proteggere i miei dati, quello che dite sempre, usiamo la crittografia, che vuol dire crittografia.
Cryptosim nasconde.
Scrivere scrive in una maniera occultando il messaggio. Quindi sono delle tecniche per nascondere il messaggio che è un determinato, come dire, veicolo di comunicazione? No, un determinato dato memorizzato contiene.
Fondamentalmente è un processo di cui ho del testo in chiaro.
Applico.
E le procedure per ottenere del testo cifrato testo cifrato che non è comprensibile, per poterlo comprendere devo fare il procedimento inverso.
Quindi dal cifrato, ottenendo essenziale il processo di trasformazione, viene detto cifratura.
Da un lato all'altro l'operazione duale decifra dura e ovviamente non è solo presente messaggio e procedura, ma esiste un'altro input che viene chiamata chiave.
Quindi la chiave è un input particolare che guida il processo di cifratura e lo conduzione ha chiavi diverse, ovviamente o prodotti di cifratura di cifratura diversa. La chiave veramente brutta.
L'algoritmo è la successione dei pasti per poter effettuare l'operazione di cifratura o decifratura. Sono delle regole e la chiave è una successione di cifre di singoli di caratteri che fondamentalmente rappresentano un secondo input di questi algoritmi e guidano il processo.
La chiave è un elemento fondamentale, mentre l'algoritmo di cifratura è pubblico, non è segreta di tutti.
Danno il testo a essere per strada. Quali sono i passi lavorativi? La forza degli algoritmi di cifratura è relegata alla chiave chiave, che quindi deve essere segretario in multipla.
Sì, è difficile da indovinare.
Il problema non è impossibilità di rompere il cifrare il problema di accedere al testo in chiaro senza avere la chiave, il problema è che per poter fare quest'operazione di rottura ci vuole molto tempo.
Il tempo utile?
Per fare queste operazioni si parla di anni, perché devo devo provare?
Quindi la qualità della chiave è il grado di robustezza della stessa all'essere indovinata.
Quindi più faccio lunga la chiave più difficile da indovinare.
Un po' come anche il meccanismo delle password.
Della password è troppo facile la indovinano subito se è una password complicata, lunga, con caratteri speciali ma in misura è minuscolo, ovviamente fare gli attacchi di forza bruta per indovinarla.
Ovviamente in base al tipo di chiave che noi abbiamo delle chiavi che impieghiamo nel due algoritmi classifichiamo sul sistema di cifratura in chiave asimmetrica.
Dove i messaggi sono Civati e decifrati, impiegando la stessa chiave.
Quindi ho un'unica chiave.
Che viene utilizzata nei due algoritmi.
Il gli algoritmi di cifratura hanno il vantaggio di essere molto veloci.
Quindi da un punto di vista dei tempi che funziona sono gli algoritmi preferiti per la velocità, però il problema fondamentale è proprio la gestione di questo segreto.
Alis e Bob devono comunicare, devono conoscere la chiave e quindi in realtà devono avere un canale laterale.

Per far sì che si accordino sulla chiave, si scambino questa chiave e lì poi avremo il dolore.
Come faccio a scambiare la chiave?
Anche perché se la chiave diventa esposta ai che il mio attaccante, perché tutto l'algoritmo crollo, perché l'attaccante conosce la chiave, non dice il fatto.
Quindi è importante che i due interlocutori abbiano un modo per scambiare e ci sono tanti protocolli di scambio chiave.
Se invece noi abbiamo due chiavi, una usata in un algoritmo.
L'altra usata nell'altro algoritmo, partiamo 10 fra i asimmetrici.
Il soggetto, quindi ogni entità che interagisce veramente. Qua parliamo di come dire emittente e destinatari, però se il dato è memorizzato il lettore scrittore, il concetto è lo stesso, però ogni soggetto deve avere una coppia di chiavi.
Una birra ci darà dei messaggi, uno per decifrare gli stessi.
Quindi se poco vuole mandare all'adis un messaggio è sufficiente che i russi. La chiave pubblica di ALIS?
Perché poi?
Con quella chiave.
Di ALIS potrà decifrare vedete, già in uso termine pubblica perché nelle due chiavi una generica.
Cerchi.
L'altra diventa un mese di rete.
Quando quella disponibile a tutti è impiegata per cifrare e l'altra, il segreto?
Parlante 1 00:08:54
Partecipare.
Parlante 2 00:08:55
Sto realizzando la confidenzialità.
Che poi è lo stesso proprietà che noi abbiamo come digitrati simmetrici.
Io voglio scrivere a Bob, prendo la sua chiave pubblica, la vado a usare per la cifratura solo Bob che ha il segreto, quindi la chiave privata, potrà accedere a quell'informazione, cioè se il computer.
Però se io inverto lo schermo.
E io vado a usare la mia chiave privata per cifrare i messaggi? O non ripudio e autenticazione perché solo io posso aver generato il messaggio? Perché solo io ho conoscenza della chiave privata. Quindi la crittografia asimmetrica mi dà due vantaggi in base a come uso la coppia di chiavi ho più della proprietà di confidenzialità.
Dice perché sono un po' più lenti.
Estremamente lento.
Quindi alcuni algoritmi, vedrete una commistione dei due.
Scambio le chiavi con la crittografia asimmetrica quando devo invece mandare i messaggi, uso la crittografia asimmetrica con le chiavi scambiate con quella simmetria. È quello che fa SSLTLS ha molti algoritmi.
Buonissimo.
Ovviamente, un aspetto importante della crittografia asimmetrica è rendere pubblica una delle due chiavi.
O me lo posso fare con infrastruttura viene chiamata pikaiana.
Il, l'identità e la chiave pubblica vengono in caso isolati in un artefatto elettronico. Viene chiamato certificato digitale.
Certificato digitale, è un documento che attesta l'identità e Lega l'identità ha una chiave?
E chi emette quel certificato viene chiamato certification Authority.

Nel certificato digitale non troviamo quindi negli attributi d'identità della chiave pubblica, ma anche l'informazione dell'autorità che ha rilasciato per certificato.
E ovviamente la firma digitale di quel certificato.
Legge Actification Authority ovviamente rilasciano le identità e poi iniziamo a vedere il concetto di identità digitale che potremmo.
Però è un modo per attestare che io sono figlio di essere nel mondo digitale.
Ovviamente non c'è un'unica soluzione, pubblication Authority per tutto il mondo non avrebbe, quindi c'è un'organizzazione gerarchicamente.
Quindi io chiedo l'identità a una certification Authority la cui identità è certificata da un'altra certification Authority.
Fino a creare una gerarchia con.
In testa una luce fertile.
È l'unica del diritto alla storia che firma la logistica e rappresenta la radice di fiducia.
Parlante 1 00:11:42
Di questo gerarchie?
Parlante 2 00:11:44
Quando, per esempio, navigate in queste tre o se ci riuscì?
Vi apparirà un lucchetto, se cliccate vedete il certificato digitale.
DS 3 1 quelle nuove organizzazioni registrazioni.
OK.
A digitalmente so già l'abbiamo detto, però a differenza della crigiografia, noi abbiamo un'altra tecnica che prende il nome di steganografia.
Sempre grafia, quindi sempre una scrittura.
Però a differenza non è più non si può forte. Che hanno scoperto.
La differenza è che mentre nella crittografia occultiamo il dato, ma vediamo l'esistenza del dato quando cambiamo un messaggio crittografico.
Vediamo oggettivamente che c'è un messaggio, ma non ne comprendiamo il significato, nella sticonografia andiamo ad occultare non solo il messaggio ma anche l'esistenza stessa del messaggio.
E quindi non facciamo capire che c'è una complicazione.
Fondamentalmente l'idea di identificare dei Cover data, ovvero dei dati apparentemente innocui entro cui capsulare dello Stato.
Ovviamente il messaggio confidenziale, non vogliamo che i frutti.
Però io ti mando un file per passare un audio.
È all'interno di quell'audio che è nascosto il messaggio, quindi fondamentalmente il processo steganografico è un processo di.
Di incapsulamento di un dato dentro un'altro.
È una delle possibili tecniche di radiografia digitale. È quello delle dalla LS and quindi list.
Significa fondamentalmente come funziona. Io prendo il file che dovrebbe contenere il mio visualizzato e vado a modificare.
Gli ultimi video.
Orzo, quindi presente, prendo l'immagine.
Immagine, ogni pixel ha una GB.
Vado a prendere gli ultimi.
2.
E invece di avere il valore originario del fatto 0 0, vado a prendere il bit che rappresenta un il dato che voglio gustare.
Questo fa sì che in realtà il messaggio tra il messaggio originale, l'immagine originale.

L'immagine steganografica.
L'occhio umano non vede una vita.
Se io però vado a fare una differenza, quindi proprio una sottrazione bit a bit, vedete che c'è una mappa, lo si vede bene dal proiettore, ma trovate dei puntini.
Quei puntini rappresentano le informazioni stregano grafiche, quello che ho aggiunto.
È sicura la streganografia fintanto che.
Non applico queste tecniche di detection.
E se only un'immagine originale o l'immagine seconografica, facendo il confronto riesco a capire che qualcosa è stato aggiunto e quindi posso capire anche che cosa è stato aggiunto e ricostruire un messaggio originale.
Steganografia e crittografia molto spesso viaggiano anche insieme, perché è possibile che il messaggio che integro nella povertà ha subito un processo crittografico alla radice.
E quindi?
Posso identificare il messaggio, ma grazie alla crittografia quel messaggio non è esposto da questi algoritmi di sottrazione, se vogliamo, quindi io posso rilevare che c'è dentro il contenuto, ma non esattamente qual è il contenuto.
Perché ovviamente la crittografia ha occultato il messaggio fino al progetto del.
Un processo crittografico è un processo è un protocollo crittografico è un protocollo, un algoritmo, una serie di regole delle procedure che fondamentalmente implementano un aspetto cruciale per la sicurezza di un sistema e lo fanno utilizzando delle primitive crittografiche.
Quindi, ad esempio, un protocollo crittografico può essere SSL che ha come obiettivo di sicurezza quello di fornire un canale sicuro.
Land Shake i messaggi. Io vado a scambiare l'operazione e vado a fare per realizzare quell'obiettivo, di avere un cane. Di sicuro quello è.
Ora i protocolli crittografici vengono formalizzati. Quindi quando voi studiate per esempio SSL, Vedrete manda il messaggio a all'elaborazione, un'altro messaggio B fra l'elaborazione e via discorrendo. Posso andare a fare una specifica formale di questo protocollo? Se ho una specifica formale, posso fare anche una valutazione formale.
Il protocollo X riesce a ottenere la proprietà di sicurezza Y.
Quindi andare a verificare se è possibile che il protocollo venga bypassato, abbia delle vulnerabili, questo lo posso fare in maniera formale.
Lo vedremo in una lezione?
Ovviamente per poter fissare gli aspetti formali.
È necessario, almeno in maniera forte, definire qual è il modello della di esecuzione, ovvero il modello dell'attaccante, cioè dato il protocollo dato l'attaccante, io formalmente voglio dire che in quel contesto di attacco c'è protocollo.
OK, uno dei modelli di attaccante viene chiamato dollari.
Modello in cui l'attaccante è un'entità attiva, può osservare, modificare, eliminare i messaggi della rete e la crittografia viene considerata perfetta.
Ovvero i protocolli crittografici non hanno vulnerabilità, non c'è possibilità di compromissione degli della Primitiva crittografica.
Quindi la verifica formale di un protocollo intellettuale testo è verificare se.
Esistono delle azioni dell'attaccante tali che il protocollo è crittografico non realizza il suo obiettivo.
Quindi se io se vado tanto è accettabile messaggi ovvero quello.
Parlante 1 00:17:45
Che mi hai?

Parlante 2 00:17:46
Scambiato sulla riga posso compromettere quello che ho crittografico, senza però agire sulla parte bibliografica.
Perché per me la parte crittografica viene assolutamente.
Ci siete?
Difficile.
Il contrattare della crittografia è la criptoanalisi.
Progresso.
Una New yin non vergogna, vuol dire sconforre anche altro.
Anche arabo.
Sì, lo so, molte.
Quindi analizzare vuol dire scomporre la criptoanalisi è bucare dicifrare ovvero posso adottare delle tecniche tali che.
Se non ho.
Parlante 3 00:18:33
Le autorizzazioni riesco ad accedere messaggio non avere l'autorizzazione?
Parlante 2 00:18:37
Vuol dire non disporre della chiave che se ho cifrato.
Ho un cifrato e non ho la chiave.
Voglio consentire la decifrazione indipendentemente dalle mie conoscenze.
È un arabo che ha formulato le prime soluzioni di criptoanalisi.
Non lo trovo.
Piaceva il testo arabo.
È il metodo dell'analisi delle frequenze.
Quindi, e lo vedremo come cripto analisi sul centro di Giulio Cesare.
Ok, no, tra poco no, ci vediamo uguale.
No, nella.
Dantesco. Abbiamo parlato di firme digitali, firme elettroniche. Molto spesso la crittografia viene creata, viene utilizzata come proteggere i dati, per proteggere le informazioni, quindi per la confidenziale.
Può essere utilizzata anche per meccanismi di. La firma elettronica. La firma elettronica, iniziamo un po' il diritto è il modo con cui siglare e dare valore legale a un documento informatico.
La normativa di riferimento per tra parte di identità digitanze per il digitale viene chiamato Edas. È un regolamento del 2016 che definisce per questi aspetti che è fondante per la sicurezza legale. È in realtà un regolamento.
E anche se era il 2016 è in revisione, quindi stiamo attendendo ai da studi in ambito italiano.
È il codice dell'amministrazione digitale.
Del card che fondamentalmente decreta tutti gli aspetti di documento digitale, tutele per i documenti digitali, tutele di trasmissione e conservazione dei documenti digitali.
I documenti devono essere firmati, noi generalmente quando abbiamo dei documenti in contanti li dobbiamo firmare.
E perché dobbiamo firmare tutto per?
Fornire da un punto di vista legale un valore.
Il documento viene firmato perché la firma serve a identificare chi ha redatto quel documento.
Quindi firmando un documento ne prendo la paternità.

Non solo, firmando il il documento AUTORIZZO o esprimo consenso al contenuto del documento.
Quindi sono concorde, concordo con quanto c'è.
Parlante 1 00:21:00
Scritto in quel momento.
Parlante 2 00:21:02
In molti ordinamenti per avere valore legale il documento deve essere firmato.
Quando comprate casa firmate il contratto, quando avete degli atti formali dovete sempre firmare. State dando valore legale a quell'azione a quel documento.
Inoltre la firma serve anche a tutelare in caso di controversie.
Se io ti vendo una causa e poi qualcuno dice no, quell'atto di vendita non è valido, io devo verificare se la firma è corretta.
Se è stato apposto sul documento?
Che è stato visionato dal firmatario.
Però in quel documento non ho avuto.
Ci siete?
Difficile.
Parlante 4 00:21:49
Dico, ci sono delle dei casi borderline dove pure se lo firmi poi si viene a scoprire che.
Parlante 2 00:21:56
Devo dimostrare.
Quando do valore legale a un documento firmandolo deve dimostrare che non sono stato io.
Ovviamente devo anche avere un meccanismo, quando io firmo giungo il rischio di cromo.
Perché? Perché se qualcun altro appone la firma?
Posto mio, io posso anche dimostrare, guarda, stanno nella mia firma.
Le firme così?
Consigliera, molto difficile imitare perfettamente la firma di un'altra persona o la grafia di un'altra persona.
Questo è un elemento dici?
Ricordo di me.
Ovviamente quando un documento è digitale, veniamo alla suggestione di Twitter, come lo firmiamo?
Diciamo in ambito, quando si è dematerializzata tutta l'amministrazione, legislatore si è posto questa domanda, stiamo dematerializzando tutto?
Ma come?
Posso avere un corrispettivo della firma autografa per i documenti digitali?
Il documenti digitali che per loro natura hanno delle caratteristiche particolari.
Posso modificare il file più facilmente?
In un elemento cartaceo non è così facile da modificare, quindi ovviamente anche la firma autografa che non è replicabile.
Cioè un digitale di tutta la vita.
Tutto è trasferito, è magico.
Quindi il codice dell'amministrazione di libritalia ha avuto come propri obiettivi quello di.
Fornire i documenti digitali.
Una validità probatoria, una validità legale equivalente.
A quelli cartacei, quindi non potevo sostituire al mio piatto cartaceo come un Titano, che non avessi avuto le stesse garanzie di normative.
Quindi nel 2018.

Si è disciplinato il CAD, quelli che sono i requisiti per avere il valore probatorio, il valore legale.
Per avere valore probatorio, un documento digitale deve essere assimilabile a.
Parlante 1 00:24:06
Una scrittura privata?
Parlante 2 00:24:07
E quindi deve avere una un'efficacia sanguina dall'articolo 27 0 notevoli del.
Codice civile.
Che cosa ci dice che prima di tutto.
Una scrittura privata?
Qui nell'idea di prova, quindi deve provare la provenienza delle dichiarazioni, chi è che sta facendo quelle dichiarazioni?
Chi l'ha sottoscritta, quindi chi ha accettato quelle dichiarazioni?
E deve essere riconosciuta la prova di non modificabilità di queste valutazioni, di queste considerazioni.
Altri eventi si incontrano, la querela di.
Il documento informatico, per avere valore probatorio, deve essere immodificabile.
È la natura stessa del provvedimento. Meglio, non è una scrittura privata.
Devo quindi garantire per il documento digitale tutta la qualità.
L'integrità e la sicurezza.
E la tecnologia deve dare ovviamente una.
Una misura tecnologica per garantire queste proprietà?
Ovviamente devo garantire che il documento è correttamente prodotto e che all'atto della firma non può essere più modificato.
Se viene modificato diventa un documento non più valido.
Esistono quindi varie.
Come dire, tecniche per firmare un documento digitale.
Queste tecniche però non hanno le stesse garanzie, quindi andremo ad analizzare un po' per capire quali sono le possibilità e magari cercare di farvi capire.
Parlante 1 00:25:49
Quale termine corretto usare?
Parlante 2 00:25:51
Tra firma digitale troppo?
La firma elettronica semplice o debole sono dei dati in forma elettronica.
Con una qualche connessione logica, un'identità.
Che vengono apposti sul documento digitale.
Quali sono gli esempi di firma elettronica semplice?
Quando voi firmate sul dispositivo, quando vi arriva il Corriere?
Quella è una figura di qualità, semplice.
Oppure quando avete scansionato la vostra firma logra e l'attaccante sul documento digitale.
Il PIN del bancomat molto spesso quando vi dicono accetta il documento, metti il PIN.
Cioè fare delle operazioni oppure la combinazione di username e password.
Voi come fate ad accettare gli esami universitari?
Parlante 4 00:26:47
Vi siete autenticati su S tre voi.
Parlante 2 00:26:49
Userete quella è una firma elettronica semplice.

La firma elettronica semplice ha una validità in Italia rispetto alla firma olografa, però con garanzie estremamente limitate, c'è un problema.
Se io incollo quell'immagine?
Sono proprio io adesso.
Quindi in realtà non ha valore probatorio, cioè in caso di contesa, nel caso di.
Parlante 1 00:27:23
Un dipartimento di parole.
Parlante 2 00:27:26
Se il giudice a dimostrare.
Se quella firma è sinceramente valida?
Posso firmare un documento come, che ne so, la compravendita di un immobile?
Settando la firma sul documento notarile no, non ha valore perché troppo tempo.
Chiunque può prendere quella firma, attaccarla sul valore del documento.
Anzi, molto spesso le nostre firme sono già online.
Parlante 5 00:27:55
Purtroppo, allora, pure la domanda di Laura.
Meglio.
Yes.
Parlante 4 00:27:58
E io l'ho firmata con.
La festa?
Parlante 2 00:28:03
Sei la cronica molto frequente è proprio brutto? Detto così, film elettronica, semplicemente.
Perché quel documento di richiesta tesi in realtà ha un'altro livello di autorizzazione.
Io vedo.
Lo studente in stile e lo posso bloccare io, posso contestare mia, come dire?
Ha posto quella firma perché fondamentalmente si richiede lo studente.
Nanni, il documento digitale e io lo restituisco, quindi c'è una prova, se io.
Parlante 6 00:28:36
L'ho fatto, quindi direi che è il garante. È lei che il garante decade di questa cosa. Il professore universitario, siamo.
Noi che ci possiamo anche, occorre.
Parlante 2 00:28:44
Ed è capitato agli studenti che hanno usato la mia firma che fate la riflessione.
Devo dire la nostra.
Però io non ricordavo di avere ancora parlato di ma non avevo email su teams, non sapevo niente, li ho fatti.
Togliere la pasta?
Quindi, in caso di controversia, il giudice che deve dimostrare se effettivamente quella firma.
Troppo oltre le prove, ma forse le evidenze probatorie effettivamente con la fine.
Due sono le firme forti in ambito elettronico, la firma elettronica avanzata e la firma elettronica poitica. La firma elettronica avanzata è collegata unicamente a un firmatario.
Ed è idonea a identificarlo?
La Pinna del bancomat o la firma Olografa non è idonea a identificare il firmatario perché non è collegato unicamente a me.
Chiunque potrebbe un documento dove c'era mio figlio fare lo snap screenshot e ha ottenuto la mia firma.

Ho un collegamento logico perché essendoci il mio nome e il cognome, chi legge quella firma sa.
Chi dovrebbe essere preparato? Ma non ho evidenza, non ho prova che l'ho fatta proprio dietro.
Generalmente è creato mediante dei dati che sono sotto l'esclusivo controllo del firmatario.
Ed è anche possibile verificare modifiche al documento.
E invalidare quella firma?
Può essere utilizzata per il contratto e i documenti dell'articolo 13 50 del codice civile, ovvero tutto quello che non attende tutele crescenti.
Un pubblico ministero, un pubblico.
Ufficiale, non può usare la fea e il comunicazione artificiale della pubblica amministrazione.
Non si possono utilizzare la fea per atti commerciali di compravendita e trasferimento asse.
Tutto il resto noi lo usiamo.
Ehm.
La firma grafometrica è un esempio di fea. Quando voi andate in banca e la Banca vi chiede USA questo tablet è 1 1. Diceva non è uguale alla firma del Corriere? No, perché la Banca ha memorizzato la grafometria della vostra firma. Quindi in realtà quel dispositivo analizza la firma che vede se è uguale a delle firme che avete depositato.
In più, in realtà la Banca ha un meccanismo di identità.
Verificata, ovvero voi avete depositato il vostro documento di riconoscimento.
L'operatore di del vostro colpo e vede che effettivamente siete la persona che ha depositato quelle firme?
Un ODP ricevuto richieste è meglio, è un meccanismo di fea.
Perché magari quel dispositivo è stato registrato all'atto della registrazione, anche delle credenziali di identità. Pensate un po', uno Speed, quello è un meccanismo, in realtà non è una Feo.
Parlante 4 00:32:04
Un feed? Vedremo la scienza però se non sbaglio, quando lo fai la prima volta che devono certificare il tuo dispositivo ti mandano proprio un OTP sì.
Parlante 2 00:32:13
Le varie meccanismi di CECNS, tessera sanitaria, passaporto elettronico sono tutti esempi di fea che consentono quindi di avere un valore di firma forte.
La fea ha lo stesso valore della firma autografa, si basa su meccanismi di identificazione, creazione di firma più avanzata di una firma semplice.
L'identità del titolare viene certificata.
Questa è la differenza o la firma semplice?
L'identità certificata chi sta ponendo quella firma è effettivamente la persona collegata sulla.
Ovviamente, come con la firma autografa, posso contestare.
Che quella firma sia stata apposta per un falso, quindi, non sono io che aver firmato, però in realtà mentre nella firma elettronica semplice il giudice in ambito di Papi mentale a determinarne la validità, però è una firma elettronica avanzata, è il soggetto che accetta la firma che deve verificare.
E quando io firmo con una fea?
Ti dicevo, il documento che si deve verificare.
Se io sono tipico di essere della firma?
Ovviamente se voglio ancora un livello più alto.
Devo legare ancora più fortemente quella firma al possessore, perché se il titolare della firma non ne riconosce la posizione.

Dal momento che la firma è fortemente legata al possessore, deve essere il possessore a dimostrare.
L'uso falso di quella firma quindi, si sposta l'ambito di verifica da chi riceve il documento a chi crea soprattutto il documento.
Questa è la firma elettronica qualificata che tra le due firme forti e la più forte in assoluto.
È una firma elettronica avanzata, quindi ha tutte le caratteristiche della firma elettronica avanzata. Con l'aggiunta viene creata a un dispositivo qualificato basato su firme su certificati qualificati della creazione della firma, quindi in realtà lo spid, una firma elettronica qualificata.
Perché ha un collegamento estremamente forte con il firmatario.
La firma digitale è un esempio di firma elettronica qualificata.
Non è uno schema aggiuntivo.
Ma è un possibile modo per realizzare una firma elettronica, no?
Fatevi qualificare e sfrutta la crittografia per legare fortemente.
Possessore di un'identità e firma di un documento, quindi viene generato ottenendo il diages del documento e cifrandolo con la chiave privata del firmatario.
Essendo la chiave privata solo sotto il mio controllo, non posso negare di avere a posto quella firma.
La verifica è fatto proprio confrontando il da, il responsabile dal documento e quello estratto dalla firma.
Utilizzando la chiave pubblica del firmatario.
La firma elettronica qualificata non ha limiti d'uso e mentre la firma elettronica avanzata ha dei contesti d'uso, la firma elettronica qualificata la si può utilizzare in ogni contesto.
Viene rilasciata da un'autorità.
Ecco anche la differenza con la firma elettronica avanzata, la firma elettronica avanzata generalmente ha un dominio di applicazioni, viene usato solo in quel dominio di applicazioni.
Invece la firma elettronica qualificata viene utilizzata in ogni contesto perché fornita da un'autorità e ha verificato la identità e quindi ha messo insieme tutte le soluzioni.
Di verifica della firma.
La firma elettronica qualificata.
Il l'onere ricade su un soggetto che firma, non sul soggetto che riceve il documento firmato.
Per esempio per l'apertura di un corso quadra S, la firma elettronica avanzata va bene, però devo contestare se vedo il falso.
Vabbè, questi sono tutti II valori probatori. È un reparto di quello che già abbiamo detto, traffico elettronico semplice, elettronica avanzata, firma elettronica qualificata con l'elettronica.
Quando abbiamo.
Un.
Una soluzione di firma elettronica qualificata e obbligo del titolare la custodia del dispositivo di firma e utilizzare personalmente il dispositivo.
Non è possibile delegare la fine devo firmare? Posso dire Leonardo Martini, la mia carta tieni il mio dispositivo. Firma all'imposta?
Questo non è consentito.
Oppure delegare a terze parti il passato si delega al commercialista.
La delega è possibile, cioè io dico nel documento.
Delego.
Firmerà lui, ma firmerà con la sua firma digitale, non con la mia.
Quindi la pef garantisce autenticità e integrità di un documento.

Però l'uso del dispositivo deve essere del titolare, è un elemento fondamentale anche per dare valore al documento.
L'uso del dispositivo da parte di un terzo invalida, l'associazione.
Di quella firma con quella identità a venire meno quelle che sono le garanzie di una firma elettronica qualificata, una firma digitale dice vabbè, ma qual è il problema?
Quali possono essere le conseguenze?
Codice penale, 485 falsità in scrittura privata.
È un reato in cui vado a alterare e falsificare una scrittura privata al fine di ottenere un vantaggio per me per te o un danno per te.
In realtà questo era il reato prefigurato anche quando, come dire, si scrive nella dichiarazione di laurea, poi si fa la firma, quindi della droga.
È un falso scritturale in privato.
In realtà è stato depenalizzato, quindi non è un reato rovinare è solo un reato. Mi piace un'ammenda.
Parlante 7 00:38:47
Ci sono delle conseguenze, queste dimensioni?
Parlante 2 00:38:52
Recentemente in realtà questo articolo è stato sostituito dal 491, ho visto sempre 400 penale per falsità in documento informatico quando Altero un documento informatico il reato viola tra i 10 anni.
Oppure frode informatica 640. Quando voi personate qualcun altro.
Entro nel registro del docente, mi metto i voti?
Prove informati.
Parlante 4 00:39:25
Però ho una cioè perché se non sbaglio qualche anno fa c'era la truffa dell'ospite, nel senso che.
Posso avere più spid con gestori differenti ricordo?
E mi ricordo che fecero vedere al servizio da qualche parte che quando c'era questo fatto del bonus 500 € io non potevo diciamo crearmi un'identità digitale con un'altro fornitore di spid e usufruire di questi e rientra sempre in questo modo informatico.
Parlante 2 00:39:55
In realtà, quando uno.
Parlante 6 00:39:56
Come ho detto, troppi dettagli.
No.
Parlante 2 00:40:02
Diciamo che quando lui dice uso, lo spinge in un'altro. Non è storia informatica, ma è appropriazione di energia. Appunto l'identità. Io già a 494 sempre codice penale, questo è stato penalizzato, quindi è un reato penale. 3 10 anni di Trieste.
Molto spesso le firme digitali vengono revocate o sospese, sempre l'autorità emette che questi documenti può sospendere e quindi un aspetto fondamentale è capire quando si firma.
Perché se si firma dopo la sospensione dell'identità digitale o alla regola dopo la revoca dell'identità digitale, quella firma non è valida.
Perché non ho più il collegamento di partita?
È importante nella firma apporre la marcatura temporale.

Quindi in quello schema, chiudendo il documento faccio il Digest, è un ciclo diges, quello è la firma, in realtà manco un elemento fondamentale che è la marcatura temporale. Quindi in realtà quando firmo?
Lo firmo cifrando il dages del messaggio, ma cifro il diges del messaggio a cui ho concatenato la marcatura temporale e la marcatura temporale è anche l'elemento che dà validità giuridica dell'appalto soffermato.
Vabbè, ci sono atti normativi che effettivamente danno valore alla mancata.
Quando firmo vado a creare una il fatto che si chiama busta Crittografica, una busta crittografica, un artefatto informatico che contiene il documento.
E le informazioni di firma?
Tutto in un'unica entità.
Ora per la busta crittografica sempre il CAD.
Ci dice che i formati di definizione di questo artefatto devono essere aperti.
Quindi devono essere pubblici.
Non devono essere i proprietari, ovviamente se io sto firmando un documento, tutti devono poter avere il modo di mettere quel documento.
Devono essere robusti, devono tollerare compronissimo, devono detollerare subito.
Devono essere stabili, quindi se vengono aggiornati devono essere retrocompatibili, devono essere sicuri.
Non devono poter monitorare del codice che possono farlo mettere dei dispositivi che riceverlo con me.
E poi noi devono avere in mano la funzione.
La busta crittografica, cioè sono fondamentalmente di tre tipi, non so se avete mai visto una busta crittografica. Il file P 7 M è una busta crittografica e viene cifrata per mezzo di una metodologia che si chiama Cades.
Quindi la firma, la busta crittografica o firma cades fondamentalmente produce un file di settembre.
Al vantaggio io posso firmare qualunque documento che viene incapsulato in una formalizzazione P setten.
Però posso firmare qualunque documento, ho bisogno di un apposito software per aprire, quindi si dice per gustare la busta crittografica, perché se voglio leggere il documento devo aprire la busta Crittografica e accedere al documento in esso contenuto.
E quindi ho bisogno.
Di software arriva per esempio usato software di lettura di rinnovati mi aprono il p 600.
Se però devo modificare il documento dopo la firma che cosa succede?
B 7 M non consente verso niente e una volta che ho firmato quel documento non può essere modificato, se lo vado a modificare rendo invalida quella firma?
Per poter modificare il documento lo devo sbustare prendere il documento originale
Rifirmarlo rigenerare una nuova busta bibliografica.
La posizione di più firme può essere fatto o con un incapsulamento tipo matrioska delle buste crittografiche dove ognuno viene firmata da un'entità, oppure aggiungendo una lista di firme all'interno.
Parlante 6 00:44:18
Dell'acquisto.
Parlante 2 00:44:18
Crittografico al disco, l'altra tipologia di firma è pades.
Ades genera file PDF che consente la firma di soli file PDF.

Quindi ha un dominio più limitato. Posso firmare solo il PDF, però mi dà la possibilità che qualunque rettore di PDF può leggere l'appuntamento crittografico.
Consente il versioning, ovviamente.
Col documento originale la firma, il Delta di modifica è la firma di quel dente via discorrendo e poi posso aggiungere molti più firmatari che vengono messi uno sotto l'altro?
Il padre si, mi dà anche la la possibilità di una firma grafica, posso opporre all'interno del documento una parte grafica che dice firmato digitalmente?
Per i meccanismi di comunicazione Vedete HTTP? Vedete i meccanismi di comunicazione tra computer si basano su messaggi Internet, quindi è importante firmare XML. Ecco la firma sadem.
Cade sei la busta crittografica per XML definisce i metadati all'interno di un documento XML per inserire le informazioni di firma, quale cifrare è stato usato, quale metodologia di firma, chi ha firmato e poi il contenuto della firma.
Richiede 1 1 mix SLT per definire questa nuova parte aggiuntiva che viene inserita negli XML. Ogni protocollo che voi dite diamo la firma usades per la firma dei documenti?
Uno degli aspetti interessanti di eiga service, il sigillo elettronico. La firma elettronica è una è uno strumento associato alla persona fisica.
Sigillo elettronico è uno strumento di firma associato a un personaggio critico.
La differenza è che la persona fisica è una persona che richiede.
Giuridica è un'organizzazione.
Quando io firmo una persona fisica puoi associare l'identità del firmatario all'operazione di firma, quando invece firma una persona giuridica?
Non mi serve sapere chi ha firmato, mi serve sapere quale organizzazione ha accettato quel documento.
Quindi la il sigillo elettronico non è altro che la contrattare digitale del linguaggio.
E ha le stesse caratteristiche si genera del monico semplice, il distributore elettronico.
Avanzato il titolo elettronico qualificato delle stesse caratteristiche.
Va bene?
Domanda.
Parlante 8 00:46:50
La seconda domanda tipo, oltre al ai modi per mandare le firme tipo ha detto PDF o l'X ML mo ci sta anche json?
No, è nell'opening di Connect. Per esempio ho progettato le backend dello Speed.
Parlante 2 00:47:07
Come cioè come XML ha dei colleghi son DJ son è altro che una semplificazione dell'X M ling prende un po' di ridondanza sintattica quando c'è stato inteso un'Africa con una cosa simile a xades nell'ambito g sono con tutte le regole di semplificazione di incendio.
Parlante 8 00:47:25
Perché ho dovuto fare un passaggio da tutto il protocollo con l'asserzione XMLA Json ristrutturato da capo per questo?
Parlante 2 00:47:33
C'è sempre il concetto di introduco nel J son delle dei tag.
Buonanotte, informazioni di firme.
Però ovviamente devo seguire le la sintassi.
Sì, Salve, è una forma.
Sadescese.
Parlante 8 00:47:50
È compresa con me, sì.

Parlante 2 00:47:54
Allora l'amministrazione digitale ovviamente richiedeva.
Il nome del digitale, come proteggere il documento digitale come trasferire il documento digitale? Un aspetto di sicurezza dei dati è sulla trasferimento.
Come trasferisco io i dati?
Ovviamente con la col finestra.
In generale, quando noi comunichiamo, mandiamo i messaggi di posta elettronica, ci siete e abbiamo studiato a reti, qual è?
Le caratteristiche della posta elettronica.
Ehi, cortana.
Siano.
Posta elettronica è affidabile?
Non è affidabile, si possono perdere i messaggi.
Ma.
Parlante 4 00:48:41
È.
Sicuro e io ti ho detto affidabile.
Parlante 2 00:48:47
Cioè, se io mando l'email con l'antidoto che arriva.
No.
Parlante 4 00:48:54
Se l'indirizzo del destinatario non esiste, la mail non, cioè ti viene, come dire?
Parlante 2 00:49:00
Hai fame, torna indietro.
Parlante 4 00:49:03
Mika c'è su Gmail, almeno così funziona.
Parlante 2 00:49:07
Allora è un meccanismo, si basa su tcp, quindi la comunicazione sono.
Però sono comunicazioni tra entità, quindi ha una garanzia di affidabilità link by link non end toend. Quindi se io per esempio io scrivo l'email lo mando al mio gestore, il mio gestore lo mando al gestore del destinatario.
I pezzi sono garantiti.
Ha senso? Succede qualcosa al mio gestore, la comunicazione non è gradita. Mi può tornare indietro? Non mi arriva neanche nessun messaggio.
È affidabile fino a un certo punto, è sicura?
No.
Chiaro, non c'è autenticazione, quindi in realtà il codice.
Inutile, vado troppo veloce.
Il codice.
Dell'amministrazione digitale ci dice, ma noi se io devo fare una notifica a valore legale? Che cosa si usa?
E se io devo notificare una multa?
Parlante 4 00:50:11
Ricevuta con raccomandata, con ricevuta di mandata, con ricevuta di ritorno.
Parlante 2 00:50:16
La raccomandata di l'ho ricevuta di ritorno è il modo per comunicare in maniera dabile e sicuro.
Nell'era cartacea qual è la caratteristica? Io prendo il messaggio e lo metto nella raccolta.

Che la posta che riceve la raccomandata è la posta darando a diventa garante, che diventa garante, che quel messaggio lo vede.
E diventa garante che il messaggio arriva a destinazione e io ho una prova ricevuta.
Che quella comunicazione è avvenuta ora, quando poi c'è stata la digitalizzazione?
Il legislatore si è posto il problema, posso garantire una comunicazione equivalente a valore legale alla raccomandata precedura di ritorno?
Ovviamente noi avevamo l'email.
Le email hanno come garanzia.
Gli stessi della raccomandata con ricevuta di ritorno.
No, chiunque può leggere dei video.
Finale, Dimmi.
Inoltre.
Non ho un valore legale e ritorno.
Quindi quando poi abbiamo costruito.
Ci vediamo, hanno costruito l'intelaiatura per la digitalizzazione, si sono posti il problema, come posso proteggere l'email?
Parlante 4 00:51:39
Ovviamente.
Parlante 2 00:51:41
Nella comunità di meccanismi di protezione dell'email già c'erano.
Perché noi per mandare l'email usiamo SMTP, giusto?
Che si poggia sul DC.
Io tolgo dcd, metto TLS, ottengo SMTPS, quindi la versione sicura di SMTP in più.
Io posso anche introdurre meccanismi di firma OE scrivo un messaggio di posta elettronica.
Come posso rendere un messaggio di posta elettronica che contiene meccanismi di cifratura e firma digitale?
La versione sicura di mime, ovvero una versione di formalizzazione.
Che il messaggio di posta elettronica dove vado a introdurre?
Informazioni del processo di cifratura e firma.
Ci Siena.
Quindi io posso rendere sicuro meccanismi di di posta elettronica o mine?
Scusate, dico Nerd Mime ESMTPS.
Basta per avere le stesse garanzie di una raccomandata con ricevuta di ritorno?
Di meglio voi legate?
Grazie.
Che cosa il garante che cos'è il garage ma.
Parlante 4 00:53:09
Non lanciate, si ha la certezza che.
Il ricevente abbia letto, effettivamente non mi interessa.
Parlante 2 00:53:16
Mi ricevente abbia letto la raccomandata con ricevuta di ritorno. A me interessa che il ricevente abbia ricevuto e poi.
Lo legge o non lo legge non è valore legale, io devo fargli una comunicazione.
Faccio un esempio, se ti arriva la multa, fatto che tu lo la Apri, vuol dire che non l'hai ricevuta.
La ricevuta indipendentemente che la Apri o meno e quindi quando nella multa dice devi pagare entro 5 giorni dalla data di ricezione, io ho bisogno.
Di stabilire quando tu l'hai ricevuta.

L'hai aperta e l'hai Letta, è un problema tuo, devi essere tu ad augurarti che quando ti arriva una comunicazione la leggi.
No, serve quindi il meccanismo di certificazione dell'avvenuta trasmissione che non è messaggio di ritorno.
Ma che io ho una catena di fiducia.
E fa sì che il mio messaggio protetto effettivamente è arrivato a te. E quando io ricevo qualcosa ho una garanzia legale e quella ricevuta abbia valore. Questa è la pec.
Quindi quando dite la pec è un meccanismo per proteggere?
Posta elettronica.
È una parte del tutto.
Io devo dare valore legale?
A quella comunicazione equivalente alla raccomandata con ricevuta di ritorno, infatti.
Non mando pec utilizzando lo stesso indirizzo tradizionale.
Ma chi fornisce il servizio deve essere autorizzato e certificato dal garante?
Quindi il garante.
Telecomunicazioni, da agid ha una lista dei fornitori di pec. Perché devo cercare il certificare il fornitore di pec? Perché per avere quella linea di fiducia devo far sì che chi gestisce il servizio abbia messo in piedi misure tecnico organizzative per garantire la protezione del sistema?
Cosa di di fornitori normali non.
Post, le comunicazioni avvengono tramite SMTPS, c'è un meccanismo di certificazione, quando per esempio mando la pec, quante ricevute ricevo?
2.
Quando il mio gestore prende in carico la mia comunicazione, quando il gestore del destinatario ha ricevuto il messaggio?
Quindi quando mandiamo la pec noi abbiamo due ricevute.
Che possono essere complete, sintetiche o.
Adesso non me lo ricordo.
Breve.
Ricevuta completa, contiene tutto il messaggio, tutti gli allegati e tutte le informazioni di presa in pace.
L'ha ricevuta breve, contiene il messaggio originale iesce degli allegati e le informazioni del Segretario.
La ricevuta sintetica, solo le informazioni presentate poi in tutto il formato, se bene.
Controfirmate dal gestore perché il gestore si prende la responsabilità di quanto sta dichiarando in quelle ricevute.
E quindi ha valore legato.
Se fate un concorso e mandate la pec?
E quando andate a fare l'orale vi dico, ma noi non abbiamo ricevuto la tua domanda?
Voi mostrate la ricevuta di consegna e quella a valore legale perché firmata da chi ha ricevuto dall'organizzazione.
Della firma digitale, un sigillo originale è una firma, una persona giuridica, non della persona che fanno.
Ci siete?
Difficile.
Tutto chiaro?
Parlante 4 00:56:56
Una domanda, ma in caso di compromissione del gestore che cosa cioè?

Posso fare le stesse rivendicazioni legali?
Parlante 2 00:57:05
Devi dimostrare che c'è stata una compromissione del gestore.
Dal lato tuo.
Se il gestore non ha ricevuto il messaggio deve dimostrare che ha avuto una compromissione interna.
Perché se io l'ho ricevuta del gestore ho la garanzia che adesso è arrivata.
Ah beh, il quadro normativo di valutazione.
Però sul risparmio sono tutta una serie di articoli. Prima di tutto questo è normato giuridicamente. L'Agid ha l'elenco pubblico e i gestori.
E fondamentalmente.
Ucciso tutta una serie di atti giuridici che fanno corrispondere la pesca a raccontato ricevuto.
E che quindi era aperto. Il meccanismo migliore per il traduttore? Con la pubblica amministrazione, però, avere valore legale delle comunicazioni.
Voi ci siete?
Difficile.
Nota.
In questo sprazzo di lezione che ci rimane parleremo della cultura, sia classe.
La crittografia si guida in classica e moderna, in base a quali sono le operazioni che eseguo per poter ottenere cifra, se sono metodi manuali meccanici stiamo parlando di crittografia classica, se invece sono dei meccanismi legati al mondo della matematica e dell'informatica.
Bibliografia moderna.
Quando nasce la bibliografia?
Parlante 4 00:58:37
Moderna 76.
Enigma.
Parlante 9 00:58:45
È stato uno.
Degli.
Ultimi meccanismi di crittografia classica propriamente ondue.
Parlante 2 00:58:57
Nasce proprio la fotografia moderna, dove si dimostra che l'informatica.
In grado di bypassare tutti i meccanismi classici e quindi ovviamente.
Nasce perché ci sono dei meccanismi di tipo analisi enigma, come è stato rotto grazie a informatica.
E quindi, ovviamente, la crittografia deve realizzarsi sull'informatica.
La crittografia classica si divide in cifrare a trasposizione, dove fondamentalmente le lettere, simboli del messaggio in chiaro, venivano trasposte.
Vuol dire spostare in avanti.
E devo semplicemente mischiare.
Secondo una determinata regola.
Perché poi inverso di quella regola mi fa risistemare le lettere o i simboli nella loro posizione originale.
Poi abbiamo i cifrati per sostituzione.
Dove vado a prendere le unità elementari del mio messaggio ben chiaro e sostituirle con nuove unità?
Che non hanno nessun significato.

Però questo mapping tra i simboli del testo in chiave i simboli del testo cifrato. Se io ci vado a divertire posso fare dopo una serie di cifra.
Oppure c'ho dei cifrari misti che combinano sia trasposizione che sostituzione.
Ovviamente l'applicazione della crittografia moderna è stata graduale.
Quindi man mano ci sono.
Sostituite le tecniche classiche, ma soprattutto man mano che l'informatica è diventata predominante.
Primi schemi crittografici.
One PIECE. Ah, cheese.
Prima.
Parlante 4 01:00:43
Ancora l'osso di qualcosa.
Posso.
Parlante 6 01:00:51
L'ingresso addirittura.
Capito?
Parlante 2 01:00:55
Mentre.
Parlante 6 01:00:56
Nel secolo.
Sono.
Parlante 4 01:01:04
Lascita, la spartana può essere l'ascita la spartana.
Parlante 2 01:01:09
Spartana del sesso del 600, anticristo è effettivamente uno dei primi meccanismi crittografici, però prima ancora ce n'era una.
Ma hai sentito parlare dei geroglifici?
Gli antichi egizi usavano una.
Parlante 8 01:01:26
Tecnica Cristografica.
Parlante 2 01:01:27
Ma anche i sumeri, diciamo.
E la crittografia usata nel secondo millennio avanti crisi in Cristo era la sostituzione di singoli standard con altri che sembravano.
Vivere sbagliate.
In realtà non era uno sbaglio di struttura.
Ma perché c'era un significato nascosto, solo chi aveva la conoscenza adeguata poteva accedere a quel significato nascosto.
E quindi era un modo per nascondere dei messaggi. E quindi è una tecnica bibliografica.
Vabbè, io vi ho messo un geroglifico.
Ti piace l'Egitto, quindi in passato?
Che dilettavo con la legge.
Per ognuno ha le proprie.
Vabbè, questo è un.
Parlante 4 01:02:18
Geroglifico, cioè lei capisce cosa c'è.
Scritto.
Parlante 1 01:02:22

Mi sono dimenticato di niente.
Parlante 2 01:02:25
Però questo era un questo è un esempio molto famoso di scrittura geroglifica con crittografia.
Non posso riesce a ricapire, non lo comprendeva tutto.
Questa scrittura vuol dire due ha due significati.
Però se mettete insieme i vari termini non ve lo.
Parlante 10 01:02:45
Pronuncio, perché non lo pronuncio?
Parlante 2 01:02:47
Però se lo leggete letteralmente i primi due singoli, se non si infilano il movimento, poi c'è un geroglifico del maiale, anche quella di destino e dell'avvoltoio e di stella, quindi se lo leggete letteralmente vuol dire il destino nasce dalla madre celeste, quindi dalla monastero.
La persona umana lo leggeva letteralmente e quindi aveva quel significato.
Però in realtà chi aveva conoscenza?
E sentiva la fonetica. La fonetica era assimilabile a la stella si muove e procede.
C'è un significato su quei due singoli che si fondono in un unico simbolo, se voi leggete la fonetica, quindi se lo sapete pronunciare.
Leggete un'altro significato che è quello reale, autentico, quindi per gli antichi questo era un esempio di scrittura enigmatica.
Enigmatica vuol dire indovinello sempre da te. Vuol dire che voi quando vedete il testo, se avete conoscenza, riuscite ad accedere non solo al significato banale ma anche al significato che c'è dietro, però dovete avere quella conoscenza.
E la Bibbia è piena di scritture enigmatiche. Quindi Bibbia prodotta millenni? No. Molte persone sono impazzite per trovare i significati enigmatici.
Alcuni, per esempio, sostituiscono ai caratteri della Bibbia i numeri e dai numeri fanno delle ricostruzioni a ritroso per trovare quel significato profondo. Non è una vera e propria crittografia, in realtà è un modo per nascondere un messaggio dentro o una funzione della crittografia e stefanografia.
Zero metodo crittografico è proprio la cittàla sparlana che è stata descritta nelle vite parallele da brutta acqua.
Parlante 4 01:04:46
Ce lo leggete? Sì.
Parlante 2 01:04:48
Magari sì.
Vengo lì?
Però in realtà lascitala era un meccanismo per mandare ordini che avevano un valore militare. La crittografia nasce in ambito militare fortemente in ambito militare, perché ovviamente i comandi militari dovevano essere nascosti, altrimenti se intercettati io sapevo il nemico cosa faceva.
La descrizione è molto semplice, si fabbricavano due bastoni perfettamente uguali.
Per lunghezze e spessore.
Aveva una forma ottagonale e si riponeva una pergamena lungo il bastone.
E poi si andava a scrivere verticalmente.
Quando poi si srotolava otteneva un testo non comprensibile, se non quando riarrotolavo la pergamena e torno a un bastone e quindi riemergeva intorno.
Messaggio quindi era importante fabbricare due bastoni esattamente uguali e che i due comunicanti avessero i due bastoni.

Crittografia chiave simmetrica.
Due elementi uguali sulle due entità.
Un'altro esempio è il quadrato scacchiera di polibio che nasce da questo storico greco, è autore di un testo, si chiama storico, che rappresenta un'idea distruzione dello sviluppo del Mediterraneo intorno al secondo secolo. a.C. Nelle comunicazioni militari. Ovviamente se io devo comunicare a lunga distanza cosa posso utilizzare? Le fiaccole.
Quindi posso usare segnali di fumo? Il problema è che i segnali di fumo potevano veicolare dei messaggi.
Limitati.
Immaginate il linguaggio morsa.
L'idea è poi quella che è stata.
Polizio nel suo capitolo descrive un metodo in cui lui codifica qualunque messaggio.
Come segnali di fumo, come funziona?
Fondamentalmente organizzava l'alfabeto in una in un quadrato.
E quindi ogni lettera 24 dell'alfabeto greco, 25 dell'alfabeto latino potevano rientrare questa scacchiera, 5 per 5 e ogni lettera era identificata dalla posizione sulla scacchiera. Quindi se io volevo dire a bastava dire uno o uno.
Ogni torre militare aveva in realtà due file di torce.
A sinistra e a destra, quindi il gruppo a sinistra rappresentava le righe e quindi ne avevo 5 potenzialmente da attivare.
Quella a destra, la colonna, quindi se iodovevorappresentare.ca SA facevo 13114311.
Quindi scendo una torcia a destra e una sinistra, quella al centro.
Una torcia e tre quelle a circostanze, una è, una è là e via dicendo in base al numero di torre, cioè sul lato destro e sul lato sinistro. Effettivamente riuscivo a comunicare qualunque informazione.
Il cifrario però più famoso è il cifrario di Giulio Cesare, quello che fu ritornato intanto.
Prendi il nome da Giulio Cesare e prescritto nel de Vite Celeste Tonio ed è usato nella guerra in Gallia. Descrive fondamentalmente che Giulio Cesare spostava quando scriveva il messaggio ogni lettera di tante posizioni più avanti dell'alfabeto, quindi se io devo mandare la c, lui non scriveva La c, ma diceva OK, partendo dalla c sull'alfabeto.
Sposto K posizioni.
Quello diventa il simbolo del cifrato io del testo cifra. Quindi alla a corrispondeva la D alla B alla e alla C alla F perché il numero di posizioni che Giulio Cesare USA la era tre. Però ovviamente quel numero 345 rappresentava la chiave.
Per determinare il processo di cifratura.
Quindi lo vogliamo rappresentare il il simbolo del testo cifrato era il simbolo nel testo in chiaro più K modulo 26. Stiamo facendo il nostro alfabeto tradizionale. Se invece devo decifrare il simbolo del testo cifrato meno K modulo 26, ricordandovi sempre che i singoli hanno un cospetto matematico tramite la tabella h.
Un modo per realizzare il cifrario di Giulio Cesare è utilizzare la macchina di Alberti. La macchina di Alberti sono due dischi sterzati da un perno, uno fisso e l'automobile.
Generalmente il disco esterno è fisso, il disco interno è mobile, quindi all'inizio faccio corrispondere a con a, poi ruoto il disco interno tante volte quanto è il valore di K.
Fisso, poi due EO è in corrispondenza, quindi questo è un modo per aiutarci effettivamente a realizzare il cifrario di Giulio Cesare.
Abbiamo parlato di.
Criptoanalisi, il cifrario di Giulio Cesare è un cifrario mono alfabetico, ovvero.

E semplicemente una rotazione della macchina al Verdi e viene ad applicare per tutto il messaggio. E se noi riprendiamo quel testo arabo sulla cripta? Analisi rompere il cifrario Alberti è molto, scusatemi il Cifrario Giulio Cesare. È molto facile. Perché? Perché in generale le lingue sono caratterizzate da una frequenza nell'uso delle lettere.
Bene, qui vedete per esempio l'italiano la 10,30, B, 0,9 la i 11,6. Ci sono alcuni alcune lettere che vengono usate più frequentemente rispetto all'altro. Ovviamente ogni lingua ha una sua specificità nella frequenza dei termini, però il cifrario mono alfabetico fa sì che queste frequenze rimangono anche.
Nel testo cifrato.
Episea la EO associato.
Se alla e ho associato la H.
Te la e sì.
Come dire, è la lettera più frequente nel cifrato. Sarà la h la lettera più frequente. Quindi, per come dire, rompere il cifrario di Giulio Cesare, Basta identificare qual è il simbolo più frequente.
E corrisponderlo in quella lingua al simbolo più frequente, vedere qual è la loro distanza.
Quella sarà la chiave K che mi consentirà di decifrare il messaggio cifrato, decifrare Giulio Cesare. Ora, se invece vogliamo avere un cifraio che non sia più robusto rispetto.
Al la criptoanalisi dell'analisi delle frequenze siamo un cifrario di vigenère.
Questo cifrario, il primo esempio nel Cifrario poli alfabetico, vuol dire che.
Per ogni simbolo che devo sostituire faccio una rotazione.
Quindi in realtà come chiave non ho un numero di rotazione fisso, ma una parola.
Questa parola mi dice quante votazioni devo fare ogni volta che devo cifrare un simbolo, quindi in realtà quel simbolo avrà più.
Rotazioni.
Ecco che andando a fare più rotazioni vado a rompere.
I meccanismi di frequenza.
Delle lettere all'interno di una lingua.
Ci siete?
Difficile.
Quindi in realtà la rotazione dipende dalla chiave.
E quindi è diversa per ogni simbolo.
Il Cifrario Vigenère rappresenta a tutti gli effetti un cifrario a chiave simmetrica, perché ovviamente questa chiave deve essere nota a entrambi.
E deve essere mantenuta segreta, perché se viene esposto ovviamente posso ricostruire.
Ho un flusso deterministico di cifratura applicando la stessa chiave, ho sempre lo stesso cifrato a partire dallo stesso testo in chiave.
Ed è un precursore dei Stream Sider moderni che utilizziamo attualmente.
Per rompere il la dipendenza della lingua, ovviamente ci sono altre tecniche.
Ad esempio, abbiamo cifrati omofoni, quindi ogni lettera frequente del testo in chiaro viene rappresentata non da un simbolo di testo centrato, ma da più simboli nel senso cifrato.
Quindi omofoni vuol dire che hanno lo stesso suoni, quindi sono indipendentemente da quanti singoli aggiungo, c'ho sempre lo stesso valore.
Oppure cifrare, non simbolo per simbolo, ma coppie o gruppi di singoli.
E questo fa sì che io, come dire, ho maggior numero di corrispondenza. Quindi il testo viene suddiviso in B grammi e trigrammi n grammi e le corrispondenze non sono a livello di lettere ma lettere, ma.
Come dire, le corrispondenze sono tra dei grammi e trigrammi tra testo e chiaro il testo cifra.

Oppure posso inserire dei simboli fittizi?
Che non hanno un impatto sul significato, magari identificare dei singoli che non alterano. Quello che può essere significato o che la cui presenza non mi trasmette un'alterazione, per esempio.
La casa è invece di mettere lo spazio metto dei simboli arbitrali. Io però leggendo quel messaggio riesco facilmente a estromettere quei simboli fittizi, perché se per esempio uso la Q, la Q casa tutto attaccato, vedo che non è come dire una parola del mio.
Della mia lingua e riesco a capire che è la Q l'intromissione artificiale e quindi devo togliere.
Oppure combinare una sostituzione, decifrare il numero Cesare con una trasposizione, rimescolando le lettere.
Per invece citrare la trasposizione, noi abbiamo il quello colonale semplice, dove vado a scrivere all'interno di una matrice il testo che devo andare a trasporre. Scrivo per righe, leggo Per follow.
Quindi inserendo il testo per riga, poi il cifrato non ha altro che il valore delle colonne che effettivamente non dei colonne formazione.
Per poter decifrare riempio la stessa matrice per colonne e leggo sferiche.
Ovviamente.
Chi invia e chi riceve si deve semplicemente coordinare sulla natura della matricità.
Quante righe è fatto economico?
Oppure posso utilizzare decifrare a griglia che sono delle schede Perforate dove dove c'è lo spazio vado a inserire il messaggio?
Poi tolgo la scheda perforata, riempio il resto della matrice con delle lettere a casa.
Solo chi ha questa scheda perforata dall'insieme di caratteri che non hanno senso, riesce a estrarre i caratteri utili per il messaggio.
Una variante la griglia a rotazione, quindi io prendo la griglia perforato, lo uso a zero grani 90 ° 180 °. Faccio delle rotazioni così che ho maggiori spazi e anche maggiore variabilità nella trasposizione.
Posso avere una parola chiave nel cifrare, la trasposizione, perché ovviamente nel coloniale? Semplice, io prendo prima colonna, seconda colonna, la terza colonna, quarta parola.
La chiave sulle colonne?
Fa sì che le colonne vengono riordinate in base ai valori dei delle lettere sulla chiave, quindi.
Inserisco la scritta lungo le righe.
Assegno ad ogni colonna una lettera della chiave, poi ordino le colonne in maniera alfabetica sulle lettere della chiave.
E questo mi rende ancora più complicato, anche se magari conosco la matrice, se no non conosco la chiave. Non so poi come riordinare il testo perché quando mi arriva il messaggio.
Riempio per le colonne.
Però che cosa succede? Devo riportare le colonne nella verso giusto.
Quindi ovviamente.
Con la chiave riesco a identificare devo vedere la V.
È la prima colonna del destro in chiaro, ma la B è la penultima nel testo cifrato, quindi prendo quella penultima colonna, la metto sulla prima.
La EE via discorrendo. E quindi posso ricostruire quelli che sono le colonne giuste, uno dice, ma Venezia come chiave a due?
5 tentativi.
Della prima colonna con la seconda oppure inverno e vedo se ottengo il messaggio che significa?

OK.
Ci siete?
Domande.
Difficile.
Allora noi ci rivediamo giovedì.
Vedete se riuscite a realizzare il Python, questi cifrare i plastici.
Parentesi.
Con i bambini delle elementari, come ha fatto Giulio Cesare e Janel, insetti?
No, mi hanno dato anche la priorità.
Presente di.