Parlante 1 00:00:00
No, quindi buono.
Parlante 2 00:00:09
Sì, sì, martedì e giovedì.
Non cambia niente, le faccio una decisione.
Puoi chiamare?
Sono 1, 4.
Parlante 1 00:00:27
Ore queste parti.
Del laboratorio.
Diciamo un po' di cose tra di noi e.
Parlante 2 00:00:33
Poi c'erano tramite lei domani.
Una domanda, diciamo così.
Ma per il ritorno?
Mi mandi il libro?
Parlante 1 00:00:45
Grazie.
No, era una cosa stiamo un po' corretto per finire.
Parlante 2 00:00:53
Prima, vabbè, in realtà gli altri anni, il fatto che.
Finivo troppo Natale, la. La lamentela era per fare il primo appello io.
Parlante 3 00:01:02
Devo lavorare, voglio fare i progetti che a Natale.
Parlante 2 00:01:06
Scenderanno un po' le velocità, l'uscita, fare prima il progetto.
Parlante 4 00:01:11
Non vi attaccate quasi.
Parlante 2 00:01:15
La differenza con le figure? Uno diceva, perché non lo sapevano? Perché ha è andato un po' più di tempo.
Perché in inglese?
Parlante 4 00:01:26
Essendo software ne parlo.
Parlante 2 00:01:27
A Natale l'hardware magari avete bisogno di un aiuto più vicino se non ci siamo trovati.
Grazie, poi volevamo approfittare di questa opportunità che per una volta tanto son due ore.
Parlante 5 00:01:40
Che posso parlare di più?
Sembra.
Quello di lei?
Parlante 2 00:02:16
Quindi abbiamo visto un po' di elementi di crittografia.
Non l'ho detto io.
Ovviamente quando.
Moderna in realtà questo passaggio è stato abbastanza graduato, è stato graduale, perché in realtà la crittografia moderna è fortemente legata a quello che è l'informatica.
Entrerà tutto biografia classica, erano meglio.

Aspetti meccanici sulla crittografia moderna ovviamente dobbiamo.
Questo perché rientriamo fondamentalmente questa.
Etica oggi in.
Termini di comunicazione ci va via sintesi.
Per contesti in cui abbiamo avuto un progresso nell'ambito matematico informatico, quindi questo è.
Parlante 6 00:03:43
Il supporto della geografia adesso.
Parlante 2 00:03:46
La il cambio tra crittografia, moderna e classica, viene subito dopo la Seconda guerra mondiale.
Diciamo la Seconda guerra mondiale, come anche altre caratteristiche informali, che è stato un po' lo sbagliato con le nuove stelle.
Questo perché la cifratura appunto della rottura di cifrario enigma.
Cui, come dire, i paesi dell'asse si fondavano in comunicazione a dire varesato.
La inefficacia della cultura si chiama plastica.
Quello che doveva essere cifrato perfetto, è stato perfettamente complicato.
Dall'altro, ovviamente, l'inventore dell'invenzione, la diffusione del calcolatore elettronico finale che ha consentito la realizzazione di computazioni.
E la possibilità, in modo o nell'altro, di poter comprare il.
Ovviamente per forza di cosa il nostro, come dire spartiacque dovuto al fatto che io con un carburatore elettronico posso facilmente realizzare gli attacchi a forza computer.
Quelli quando noi andavano i vincoli. Decifrare il 22 cifre che abbiamo visto quanti sono i costi di combinazione di.
Giocare 26 tentativi?
Con un calcolatore quanto ci metti?
Posso farlo con un calcolatore di vendita di prima signora, però alla fine sono tempi di distribuzione abbastanza accettabili.
Noi abbiamo bisogno di andare verso delle casistiche di problemi che ovviamente sono intrattabili con carburatori, cioè il nostro metodo di riferimento è il calcolatore elettrico.
Negli anni 50 e 60, quelli di.
Cifrati vanno verso lo spettro della matematica, mi aggancio a un problema matematico, mi aggancio a una formulazione matematica che rende principale non impossibile da rompere.
Perché per poterlo rompere con l'accappa forza bruca ci metto così tanto tempo, mi diventa inutilizzabile quella ultima.
Il purtroppo e tante materie troviamo sempre scena anche in questo, cioè?
System che fondamentalmente ci dice quali sono i criteri strutturali che devono guidare alla progettazione di un cifrare. E io per per realizzare un cifrario che cosa devo garantire? Quali sono gli elementi?
Che cosa vuol dire sicurezza perfetta? E ovviamente la base poi dell'analisi protagonisti dei sondaggi.
Quando un cifrario devi uscire?
I due principi che identifica che avete magari già sentito dai colleghi, crittografia, è il principio di confusione, il principio di diffusione.
Principio di confusione fondamentalmente vile, vendere il rapporto tra testo cifrato e chiave.
Più complesso possibile, più non lineare possibile.
Se io ho più copie del testo in chiaro e del testo cifrato.
Indipendentemente da quante ne ho, non riesco a risalire alla chiave che ho generato.

Ci siete? Quindi la conoscenza delle coppie cifrato è sta in chiaro, non rappresenta una conoscenza per rilevare la chiave.
Sì o no?
Calcola che ora posso generare quante copie voglio.
Quindi potrei risalire alla chiave, questo non deve essere.
Non devo garantire una correlazione.
Tra il diritto della Giada e quello del testo centrale.
E quindi ogni variazione del video della chiave deve produrre.
Una forte variazione costruttiva proprio di una generazione, questa relazione.
Possa implementarle con operazioni di sostituzione.
Parlante 3 00:08:04
Però devo avere.
Parlante 2 00:08:05
Sempre una non linearità.
È una componente non aritmetica della sicurezza, perché ovviamente quell'elemento di imprevedibilità che comunque la regolarità tra chiamate.
Sul principio di distinzione.
Tutti dicono sì.
Non posso stare.
Chiama mamma.
Sul principio della diffusione, in realtà è legame tra il testo in chiaro e il testo cifrato che si deve, perché ovviamente devo far sì che un singolo bip di variazione un testo chiaro, mi deve comportare una forte variabilità sul cibrato e questo impedisce poi.
Di effettuare degli studi statistici.
Come avveniva sulla città del Giulio Cesare, e voi andate a vedere il centrale di Giulio Cesare proprio perché c'è una relazione lineare tra.
Il testo in chiaro, il testo cifrato io, avendo il testo cifrato.
Posso andare a bere una conoscenza?
E se vado a modificare qualcosa come aspetti, chiaro, non ho grandi variazioni.
Il testo citato mi cambia solo un pezzo, questo.
Esatto, perfetto.
I due principi ovviamente sono complementari. Devo aver rientrato.
E quindi infiltrare i moderni, si cerca di lottare delle soluzioni per avere entrambi i principi.
E in questa lezione noi vedremo il des, la SE vedremo come il des la S realizza il principio di rifiuti.
Quindi un sistema solo di fondente.
È un sistema lineare e quindi è un sistema prevedibile, non esatto.
Un problema solo confusivo?
Non maschera la regolarità di linguaggio.
Proprio del tempo chiaro, quindi devo avere entrambe proprio per avere un mascheramento molto più profondo delle informazioni.
La sicurezza di un sistema di cifratura verso.
Non dipende dal fatto che l'algoritmo è segreto?
La segretezza dell'algoritmo non è un fondamento della sicurezza di un centrale, tanto è vero che i cifrari sono standardizzati.
Quando noi parliamo adesso del des e il DAS?
Vediamo effettivamente quali sono le operazioni che si fanno.
La sicurezza è legata fondamentalmente alla conclusione delle relazioni.

Alla robustezza della chiave, all'impossibilità di ottenere.
I dati conoscendo le altre informazioni.
Ci siete?
A tutti.
Difficile.
Crittografia asimmetrica, l'abbiamo vista che cos'è la crittografia asimmetrica? Questa è stessa.
Per Alice bomb.
Parlante 7 00:11:23
Are bene la cifra dura?
Parlante 2 00:11:27
Una solo realizzate con l'associazione.
E quindi in realtà c'è un elemento di simmetria rappresentato, proprietà variante.
In generale noi studiamo i cittadini a blocchi, i cittadini di.
Pubblicità in russo non vado, vado un po' più leggero, però alla fine.
Però decifrare un blog qui è importante, andando a vedere soprattutto sufficiente.
Un'area propria, fondamentalmente il cifrario che ha un input.
Che ha o per esempio in chiaro che ha lunghezza pubblica, cioè si chiama blocchi, che lavora sul blog ci proprio, può avere una lunghezza il blocco da 64 a 256.
E applicano le trasformazioni controllabili dalle ultime cifratura sul blocco, quindi li restitui prendono in ingresso in blocco anche messaggi utilissima restituiscono in uscita un blocco e la stessa dimensione del libro più utilizzo.
Perciò tu ci trarre quello ci siete.
Ovviamente perché il simmetrico la chiave è l'attesa per le due operazioni, io devo garantire protezione.
Della trasmissione e conservazione di quella chiave.
Ovviamente posso fare il cifrario più fantastico del mondo, ma se trasmetto le chiavi in maniera insicura conservo le chiavi in maniera insicura.
Non serve a niente, tant'è vero che gli dici attacchi, no? Quelli proprio per carpire le chiavi proprio.
Voglio avere la chiave, ma.
Se poi c'è una cifra di denuncia, la chiave?
Sì.
Quindi un blocco di NB può assumere due alla n combinazioni possibili di valori finali.
Di conseguenza esistono due linee possibili e due alla n possibili output.
Qui era una funzione di cifratura, blocchi non è altro che una permutazione.
Una funzione.
Che associa a una istanza di quelle due alla m combinazione un'altra istanza delle altre due alla n combinazione.
Sì.
Parlante 8 00:13:55
Non c'è diffusione, quindi non c'è diffusione, cioè non viene cambiato il numero di bit per mutazione e no fenomeno di.
Parlante 2 00:14:02
Me quindi in corrispondenza come lo faccio? Puntando gli elementi di.
Questi due persone elementi.
Ovviamente, però, c'è un'altro aspetto.
Solo devo fare la foresta oldenza la foresta corrispondenza deve essere reversibile.

Se io cibo e poi non riesco a decifrare.
Quindi fondamentalmente, se io voglio andare a vedere quali sono le possibili corrispondenze reversibili, due alla n. Fatturiamo.
Parlante 4 00:14:42
Siamo vicini.
OK.
Sì.
Parlante 2 00:14:48
Se vado a ovviamente voglio realizzare queste corrispondenze, io dovrei prenderne blocco uno corrisponde un blocco ci troppo due corrisponde blocco due cioè dovrei fare un'alfabeto?
Che sarebbe una tabella enorme.
Perché dovrebbe avere, come dire, con blocchi di 64 bit il numero possibile degli input uguali a 64, quindi io dovrei fare 64 per due alla 64 Unione 9?
Qui non è che noi realizziamo questi centrali creando tabelle che hanno tutte le cose.
Ma devo avere una soluzione algoritmica, cioè ho bisogno di una sequenza di operazioni che mi implementano quella corrispondente.
OK.
Ovviamente questa costruzione algoritmica deve essere compatta.
Ricordatevi del naso del software, usate e cifrare i vostri implementati in hardware quindi io devo avere un'apprensione.
Su come vengono realizzate, quindi avere una certa compattezza nella realizzazione ci aiuta e poi deve essere commutabile, cioè devo avere un po' della realizzazione che ci viene accettabile. Innanzitutto troppo tempo.
Non assente.
Ovviamente entrando la memorizzazione, quindi devo far sì che questo algoritmo mi dia un prodotto e se applico il duale di quell'algoritmo io ritorno indietro.
Quindi la decifrazione del cifrato, il messaggio deve essere il messaggio di partenza.
Senza differenze, deve essere esattamente uguale.
Quindi in realtà la cifratura non è altro che una composizione di operazioni elementari, devo definire delle operazioni elementari come sostituzione permutazioni, le devo comporre in qualche modo e le devo ripetere nel tempo?
Vi faccio una serie di round.
Ovviamente.
Io ho i miei brutto, una chiave.
Chiave che dovrò applicare a queste operazioni.
Di mai usare la stessa chiave?
Va in ogni round, io uso una sottochiave di round.
Sei la stessa chiave.
C'ho una linearità.
Il tutto deve essere una sequenza deterministica, cioè io faccio sempre le stesse operazioni per ottenere sempre lo stesso da.
Il suo input deve corrispondere allo stesso auto se voi date lo stesso testo in chiave.
Terzo girato del presente, lo stesso.
E questa è una caratteristica dell'invertibilità e se io cifro un testo in chiaro vado a tenere due cifrate, come faccio a inverti?
Ho due testi in chiari, ottengo lo stesso citrale.

Sono problemi di vertigini dell'economia, quindi io ho bisogno che da ottengo B proprio per garantire che da B posso ritornare ad altro.
Ogni cifrare moderno in realtà ha una appartenenza delle famiglie di operazioni reversibili.
Nell'insieme dei propri possibili, senza ovviamente alcuna memorizzazione delle stesse, non lascia tracce.
Deve lasciare traccia, infatti io leggo quelle tracce di tutti i prodotti, riesco a ricostruire.
Quindi non cifrare i propri. Fondamentalmente si compone di due livelli.
Una parte a sinistra dove abbiamo la processazione deve essere in chiave.
Per ottenere la società con una serie di interazioni.
Con una lunghezza quindi di interessi.
Faccio una parte a destra.
Che genera a partire dalla chiave che viene fornito chiave per le varie interazioni.
Quindi ho bisogno di una definizione della parte di processazione dell'obbligo. E poi come rischio durare lo schelling della chiave come di volta in volta generare la chiave?
Da usare nello specifico nell'interazione in particolare generale.
Dobbiamo vedere come realizzare questi blocchi e ci rifacciamo a un'altro signore che è festa che è. Negli anni 60, 70 erano quasi tutti IBM, se andate a vedere lavorava BBM tutti quanti.
Comunque negli anni 60.
Realizzò un metodo per costruire il decifraggio invertibile.
A partire da funzioni, però, che non sono necessariamente.
Perché se io ho.
Una serie di violazioni.
Non funzioni affinché la totalità sia invertibile proprio che le parti siano invertibili.
Consigli.
Lui invece di fece una costruzione in cui la totalità è invertibile.
Ma non è detto che la parte elementare, le operazioni elementari, siano tutte invertibili.
Quindi qual era l'idea alla base di questo schema che viene chiamato o cifrare difese la rete di Fester.
Si divide un blocco in due parti.
Ovviamente il blocco liquido.
Parte destra, la parte sinistra d uguale lunghezza, quindi se il blog è di 643232.
E in generale il figlio si indica con l Zero R Zero quando la prima interazione è uno l'uno.
E le operazioni di trasformazioni vengono applicate su una delle due dati.
Quindi una delle due parti ha le operazioni di manipolazione, ovviamente con l'associazione.
E il processo?
Ha una ripetizione di applicatorie. Questa rete è il round, quindi a partire da l'economia -1. R con l -1 costruisco la nuova coppia.
L'economia, l'economia numero è l'economia è l'r con l -1. Quindi io quello che c'era a destra lo riporto a sinistra nella propria Federazione. Non faccio nessuna operazione di manipolazione, quello che invece era a sinistra vado a operarlo, a manipolarlo, per costruire la parte di destra. E come, che cosa faccio?
Prendo la parte.
L con l -1?
E faccio un ipsoll con una funzione F in cui do come input R con l -1 e la chiave del round.
Come fare? F, poi vediamo.
Quindi una rete di riflessive a questo schema, dove la funzione F è la funzione di RAM.
Ok.

È un incrocio con un'operazione al di là ci sono varie varianti però delle reti di test nel tempo, poi.
Come viene fatto? Quale parte viene processato? Ci sono tutta una serie di variazioni, però lo schema generale è questo.
Sì, difficile.
Il cuore del cifrario è la F.
È quello che fa la manipolazione.
Perché combina una metà del blocco con la chiave di round.
Edizione, notate che poi la chiave di round non è tanto lunga quanto il tutto reale.
Il punto reale è molto più lungo, riempito di raggiungibili rispetto alla sottochiave, servono proprio quello schermi.
Ci siete?
Attraverso una serie di operazioni di sostituzione e per amministrazione fanno sì che sia non lineare.
È difficile dai divertirsi.
Anche perché se vedete a parte FX.
Storie lineari delle storie linea della parte di non linearità è proprio la F.
Ci siete e poi lavatevi confusione.
Ovviamente in questa costruzione si dimostra che a me non serve che sia invertibile per garantire l'invertibilità dell'operazione.
Perché proprio la struttura della rete che mi consente di invertire, di disfare l'operazione di cifratura?
Semplicemente come.
Applicato ricami per fine inverso.
E io per cifrare ho usato le chiavi di round da zero AN.
Ne ha zero fino al processo, vediamo.
Quindi immaginiamo di avere il G Round e di generare da l con zero AR con zero con successive applicazioni della rete INTESTERM.
L.
Scusatemi R con TL con t solo con un'unica accortenza la parte finale.
In realtà è solo uno scambio, non è un'esecuzione della rete di feste.
Ci siete?
Difficile.
No, come posso?
Avendo R con TE le conti che è il cifrato, risalire al testo in chiaro e quindi ricostruire le con zero delle cose zero.
Uno dice, dobbiamo riapplicare.
Feste con ordine inverso delle chiavi. Questo vuol dire che in realtà nella parte in alto.
Ciao.
Che R con TR con T applico Phasel, con K con t Voglio vedere cosa ottengo a valle dell'esecuzione della rete di feste.
Ci siete?
Ovviamente LI -0 che il primo punto interrogativo non è altro che l Conte.
Quindi.
R.
Sì, perché ovviamente.
Mentre nella parte in basso ciò che R con T è in XO di FL con TK di B è l'applicazione della rete.

In questa proporzione applico.
Il y.fr di T -1 K con DA entrambi i lati della relazione LT -1 uguale a quella relazione, quindi applico 1002 operazioni.
E il dato quindi che LD uguale R con T -1.
Possiamoscriverechelotmenounoeugualea.ro T.
Il sole F che lui Confidi la qualifica.
Quindi ho ricostruito effettivamente che questa esecuzione mi ottiene quel tuo elemento.
Iterando.
Ottengo.
Ci siete?
E quindi abbiamo invertito.
La F l'abbiamo usata all'inverso no?
Abbiamo sentito l'inversione dell'operazione.
E la conclusione data dalle sostituzioni, dalle operazioni non lineari della F.
E la diffusione invece la lo scambio finale?
E la alternanza delle operazioni di feste?
E ovviamente il fatto di un lavoro su metà dei blocchi in si dividono dall'auto a mano.
Numero di round è un elemento importante perché determina il grado di sicurezza.
Più iterazioni faccio, maggiore è il livello di sicurezza, ovviamente se ne faccio uno solo.
E devo fare il numero.
Ieri voleva ottenere un livello di potenziale.
Il come dire, indipendentemente da come l'abbiamo realizzata, le costruzioni a reti di pezzi sono molto interessanti. Perché? Perché in realtà la loro costruzione di variante.
E io per fare la cifratura o la decifratura, da un punto di vista delle operazioni è sempre la stessa.
Devo avvertire solo l'ordine delle chiavi e se io devo implementarlo in AV l'APP è uno.
È la rete.
Devo solo capire il circuito di schede della chiave.
Finché vuol dire deve fornire a questo terzo di hub le chiavi, se lo dà nell'ordine crescente.
Cipro se lo dà nell'Oriente decrescente.
Reciproche, cioè da un punto di vista hardware è ottimo perché è tutto qua.
Ci siete?
Anche dal punto di vista software è interessante per la dimo la funzione sempre la stessa, quindi non devo realizzare due funzioni riciclatura e cifratura, ma la funzione è sempre la stessa, devo solo abilitare l'ordine di prodigio di chiamate.
Quindi non devo progettare due entità per delle operazioni.
È un cifrario forte perché ovviamente parte da eventi semplici e quindi è facile da studiare nelle caratteristiche.
Ovviamente ci sono un po' di criticità sulle reti di feste, la prima criticità è che devo scegliere bene il numero di round.
Siamo pochi, i numeri di round, ovviamente diventa più facile comprometterlo.
Proprio tra analisi differenziale lineare EO attacchi strutturati devo fare varie interazioni?
Se F è semplice è poco lineare, ovviamente viene meno il principio.
Confusione.
Paesi indebolisce cifrare. Quindi devo anche fare una scelta di una F.
Abbastanza di di fortemente rolline.
Parlante 9 00:28:44
Ogni round però dipende dal.

Parlante 2 00:28:47
Precedente.
Da un punto di vista hardware questo è un problema. Non posso fare il pane degli zar.
No, perché dipende sempre da quello. È sequenziale? No, nella versione.
Parlante 10 00:29:02
Una versione texture, se non.
Parlante 2 00:29:04
Sbaglio? Il testo ci dovrebbe essere, è.
Paralizzato della meglio. Dipende da sempre. Aspetta, dipende cosa poi paragonizzarlo.
Cioè io voglio per cifrare un pezzo, devo aspettare che si conta la cifra dura è per forza sequenziale.
Parlante 11 00:29:19
Però la cifra dura invece è a.
Parlante 2 00:29:22
Lui da Maddalena.
E fare dipende dalla modalità usare dipende da.
Ma su blocchi, non sul singolo.
Di quello che resteranno i modi di operatività. Quando c'ho dei dati più grandi di 64.
E quindi organizzo sotto proprio devo però quel fume uso a destra.
E io vedo un blocco e vedo il destra, lì non c'è parallelismo, ma me lo dice già la struttura.
T -2 dipende da T -1.
Come faccio andare a revisione?
Ciò questa sequenzialità nella nell'esecuzione, in realtà da un punto di vista hardware io faccio un'implementazione minimale perché lo implemento una sola volta.
E poi eseguo con circuito più volte, però non lo posso, non posso fare n istanze del circuito di lavoro parallelo, quindi c'ho dei tempi futuri.
Quindi l'occupazione dell'area è limitata, devo realizzare solo il test e il test.
E vabbè, lo scambio no, ce l'ho con un problema.
Però i tempi di esecuzione sono estremamente lunghi da un lato all'altro, non possiamo fare altri schemi, sono più caratterizzati intrinsecamente.
Tende ad avere una struttura più vincolata.
E quindi possono essere c'è una prevedibilità.
E poi ovviamente io c'ho il problema della dimensione limitata, il blocco a quella dimensione.
Ho due alla n possibilità da corrispondere a due alla n, quindi è possibile avere l'effetto problema?
Se il blocco è relativamente piccolo dopo una certa quantità di dati cifrati, è probabile che due blocchi in chiaro più distinti vengano cifrati nello stesso blocco cifrato.
E quindi?
Un po' quello che capisco, vedremo anche nel letto.
Vediamo il destro.
Il des è stato per lungo tempo prima di tutto uno standard.
Ma il centrale di riferimento per la cittadinanza?
Abbiamo 64 bit di resto in chiaro, produce 64 bit di qualche filtrato. Una chiave a 56. Vedete?
La chiave lo deve la stessa Vicenza.
Destra sta per data in funzione standard. la S fa proprio capire che è uno standard. È stato un processo di distinzione codice standard.
Per vent'anni è stato il modello di inserimento oppure è stato sempre nell'i? BM.

Ed è ufficialmente lo standard nist dal 77, che ha avuto varie applicazioni sia in ambito militare che in ambito civile.
È un cifrario blocco su reti di festa, quindi la struttura interna è una rete di feste. Lavora, come abbiamo detto, nei blocchi di 64 con chi aveva 58 di 8 bit rimanenti su un movimento di parità e quindi è la chiave.
Lo spazio effettivo delle chiavi due alla 57.
Che allora era un tempo era molto sicuro, questo perché commisurata ai misuratori che erano.
In realtà la chiave a 7 bit e poi l'ottavo bit di parità, 7 bit, ottavo il bit di parità.
In com'è strutturato? Ogni cifratura si compone di 16 rami, quindi la rete di 16 round con due operazioni di permutazione nuziale e permutazione finale ci sono una diversa dell'altra.
Queste due operazioni non hanno una valenza di sicurezza, non servono per la sicurezza.
Quindi non sono operazioni, anche perché sono delle operazioni linea, servono per adeguare l'implementazione hardware.
Il des era pensato per una realizzazione hardware in un po' processione.
E quindi ovviamente io devo avere un accorgimento.
Per implementare il des nell'hardware che era quel test?
Il problema vera l'albero è cos'è?
Ha poco potente.
Tempi blu, tempi Monti.
Leonardo e Ridati come di passaggio.
Dove viaggia la vorrei?
Circuiteria.
Sul basso suoneria.
Quante linee?
Parlante 8 00:34:51
Sicuramente non 64.
Negli.
Parlante 2 00:34:56
Anni 70 che il processore.
Parlante 8 00:34:59
Mi sembra 8.
Parlante 2 00:35:00
Ah 888.
E quindi qual è il problema? Io c'ho un blocco a 64 ma c'ho linea 8.
Che si crea un palo di bottiglia.
Eh certo, lui mi passa 8 bit, lo rimetto.
Vai agli i miei amici.
Scorri fino alla fine.
Se devo mantenere i 64 quinto devo fare un registro a 64.
Io devo fare una fila di 64 film proprio.
Parlante 1 00:35:46
Mmm.
Parlante 2 00:35:46
E che problema c'ha? Una fila di 64?
Parlante 12 00:35:52
Che se sono in serie, che se sono in serie, se se ne rompe uno.
In pratica non sono raggiungibili quelli dopo.

Parlante 2 00:36:01
Se si rompe uno.
Siamo piaciuti.
C'ho tante linee di connessione.
Io devo metterli, purtroppo devono avere le linee tra di loro.
E soprattutto, io c'ho le linee di controllo.
Più lungo è il registro.
Parlante 8 00:36:17
Più lungo, più lunga la linea.
Parlante 2 00:36:19
Quindi occupano più.
Spazio in più, ricordate le Philippe dottor Vabbè?
E questo non lo vedete, ma ve lo dico io, sono dei lesh.
Quindi ci hanno un segnale di attivazione.
Vuol dire che c'è un segnale di clock che mi dice adesso la dell'input resto dai l'output?
Più lunga è la linea.
Un segnale di blocco degrada, quindi ovviamente fare una linea troppo lunga fa sì che quel segnale degradandosi attiva degli errori, non è che il registro si rompe.
Aperto la sponsorizzazione, non sono sincronizzabili e quindi perdo dei valori.
Ovvero un flip from legge, un valore che non è quello che intendevo io di amalea.
E occupa anche un maggiore conoscenza.
In generale, quando si fanno queste architetture si utilizzano 8 registri da 8 bit, quello era un registro 8 bit più compatto.
Non hai problemi di block, no?
E quindi ovviamente è più semplice da gestire, però qual è il problema?
Io devo riempire gli 8 registri.
Quindi avevo su ogni linea un registro.
E quindi arrivava il primo bit, andava sul primo all'inizio.
Quando però arrivava poi l'altra parola e il nono bit che va su uno sul registro.
Quindi quelle permutazioni rappresentano gli ordini di arrivo.
Dei bit quando io sto utilizzando.
Basa 8 clip e 8 registri a sferimento di 8 clip.
Quindi quella permutazione iniziale modella le logiche di riempimento dei registri esporti.
Sì.
Perciò non impatta la sicurezza, è solo come dire quello che io faccio in hardware quando lo realizzo.
Dovendo gestire prof a 64 su registrato B.
Facile.
Quindi quello è.
La permutazione iniziale, l'inversione.
Parlante 13 00:38:37
Della permutazione iniziale è proprio questo.
Parlante 2 00:38:41
Ho ottenuto il cifrato, butto la prima parte subito basso, butto la seconda parte sul basso, terza parte sul basso.
Sto riequilibrando poi risistemando così che le informazioni giuste vanno di testo cifra.
Poi c'ho la l'iterazione, che è l'esecuzione ripetitiva della rete di test, sempre la stessa parte da parte sinistra, parte destra, la parte sinistra diventa.

Viene manipolata per diventare la nuova parte destra del blocco successivo. La parte destra viene ribaltata sulla destra senza modifiche.
La funzione F fa delle operazioni.
E le la la vedete rappresentate.
Ovviamente ha due input e darebbe il blocco corrente, la parte destra del blocco corrente 32 bit, la chiave di direzione 48 bit.
Ci siete?
F perché a 56 download?
Prima operazione, faccio un'operazione di espansione.
Quindi 32 bit del blocco devono andare in X oro con la chiave.
Al Block e 32 la chiave è 48.
Qua.
Quindi dobbiamo espanderlo. Quella espansione fa sì che vado da 32 a 48, ma come faccio ad andare da 32 a 48? Duplico alcuni film?
Quindi c'ho delle regole che mi dicono, Vedete quello va lì, quello va lì, quello va lì, quello va lì, quello viene replicato di là, quello viene replicato di là. Quindi in alcune posizioni ho una corrispondenza a uno a uno.
Di un bit del blocco, direi di vantaggio in un bit del blocco espanso.
Alcuni bit del blocco in chiaro, scusatemi del blocco di input vanno su due posizioni del blog spazio secondo quella regola.
Nota standard.
OK, poi faccio lo store perché adesso ho i 48 bit e quindi faccio l'ING store bit a bit.
Quindi un bitwiste?
Di.
Nel blocco espanso con la chiave.
Successivamente ho una successione, vedete se con un secondo 36456E6 con 8 si chiamano S box o substitution box, ovvero è una tabella.
Che contiene la sostituzione.
Hai l'input, un output.
Isastitution box sono suddivisi in 8 gruppi da selvit per ottenere in output quattro bit.
I sei bit vedete 101110 prendo il primo e l'ultimo è il riferimento della riga.
II. Rimanenti centrali, il riferimento della colonna.
L'elemento intersezione è valore nuovo che devo mettere in codice binario quattro bit.
Domanda, perché facciamo 864?
Perché noi dobbiamo fare substitution di 48 a 32 e noi facciamo un'unica S box?
Che ci contiene tutte le corrispondenze dei tutti i possibili elementi, 48 bit, quindi uno ha 32.
Sarebbe l'ideale.
Sempre una box di sostituzioni sembrano lineare.
Parlante 14 00:42:41
Perché l'hardware è più facile per analizzarlo.
Sono talmente più piccole.
Parlante 2 00:42:47
Tant'è vero che ne faccio 8 tappellire e quindi è più facile fare.
Uno che da 6A4E1 più gigante che da 48 per 32.
Parlante 15 00:42:59
È una questione di.
Parlante 2 00:43:02
Ci siete?

È difficile.
Le S box sono elemento di confusione, perché non sottolineare?
Ed è quello l'elemento di non linearità.
Poi alla fine non lo so.
Abbiamo una permutazione?
Quindi è un beatbox dove i 32 bit mettono un po' mesciati mossi secondo quella relazione.
E completare la funzione F.
Quindi in funzione F espansione X sostituzione per mutazione.
Permutazione p box e scansione 8 blocchi 6 4 PS box.
Ci siete?
Difficile.
No.
Ok.
Problema.
Se non avessimo l'elemento di non linearità, il nostro des sarebbe linear.
E questo ci crea un problema.
E.
Il professor Bisanti scrive, Fatto una bella definizione.
E dovevate risolvere delle sue slide, io ve le ho risposto.
Sappiamo come si fa l'esercizio.
Quindi il des per essere lineare, che vuol dire che un cifrario è lineato.
E fondamentalmente la trasformazione testo in testo cifrato usando la chiave è una relazione lineare, come posso rappresentare una relazione lineare?
Te li mando immagini.
Dopo l'operazione con matrice.
Quindi ci.
Testo cifrato, è uguale la matrice a.
B.
In store la matrice B per K, dove B è K sono testo in chiaro e la chiave.
Ci siete?
Ma cifrare è molto complesso.
Non ho aibi.
AEB è la quello che io vedo esternamente delle relazioni lineari che poi viene implementato dal cifrato.
Non è che c'è veramente aria in B, ma se io studio le relazioni, quindi ho le coppie.
PC dato K Cappella costante. Tante di queste coppie mi consentono di avere delle osservazioni che io posso riassumere o modellare analiticamente, costruendomi, Derivatrice AEB?
Ci siete?
Funziona.
In realtà io potrei anche fare che guardando queste osservazioni.
In realtà mi costruisco la matrice M.
Perché prendo le coppie BK?
E mettendole in relazione con C, mi costruisco una.
Matrice M.
OK, quindi?
L'analisi lineare, studiando le copie di testo in chiaro, il testo cifrato arriverebbe al 100%.
Di ricostruzione, perché se io ho m.

Io posso andare direttamente a fare le operazioni sia di cifratura e di cifratura, conoscere.
E la linearità del cifrario è dovuto alla linearità dell's box, si dice che la S box lineare rende il cifrario linearmente omomorfo all'operazione di ristoro.
Quindi il.
Quindi ogni round del desk è definito in quella maniera.
Essere omomorfa, l'operazione di Hipstore vuol dire fondamentalmente che il complesso è una trasformazione lineare di quel vettore.
E quindi questo mi consente di.
E quindi l'intero dress sarebbe una operazione lineare, perché la S box è lineare.
I box e linea a.
La composizione di funzioni lineare e lineare, l'intero cifradio diventa lineare.
Ci siete?
Quindi la legge Fessel non non è un elemento di non dire è proprio la S box.
La S.
E quindi fondamentalmente per estensione l'ipsore dei cifrati M1M2M3 è uguale a cifrato dell'X o di M uno, m due. Questo è l'omomorfismo nell'operazione di Xordi, ovvero io posso invertire tra l'ixor l'operazione di cellula.
Proprio perché esiste questo morfismo, è possibile determinare la matrice enne che mi consente di.
Dato.
PEC.
Costruirmi, il.
Il cifrato di P.
Ed è questo che mi consente quindi di rompere il ciclo.
Ora come costruisco la funzione la matrice m date le varie osservazioni come posso fare l'analisi?
Ora la matrice M ha n quadri BT incognito.
ECE altri enti.
Quindi io.
Per le coppie che io posso ottenere servono almeno n +1 coppie note in generale, dove n è la lunghezza.
Ma è possibile fare anche delle ottimizzazioni in questo senso, quindi se si è a disposizione p uguale a 0 2 terzo punto zero.
Civile cifrato di zero si va a ricavare immediatamente.
E quindi restano n quadro incognite per M tolgo già inizio a togliere n incognite scegliendo come testa in chiave.
Se l'attaccante può scegliere i vari plaintex e questo attacco viene chiamato Juncker Planet, basta inviare n vettori della base standard.
Vado a ottenere le colonne della matrice ella.
Perché anche questo fa sì che io rimuovere i tentativi che sono necessari per la performance.
Sulla parte di generazione delle chiavi, quindi non è bene che si allineano essere non viventi.
Per lo scheduling io ho una chiave a 56, devo fare 16 round, quindi ho bisogno di 16 sottochiavi e ogni sottochiave è fatta a 48.
Questo è lo schema per la generale.
Quindi inizialmente la chiave è permutata in C -1.

È divisa in due parti, 28 e 28, quindi la parte destra e la parte sinistra. Ad ogni round vado a ruotare ogni porzione di uno e +2.
Sì, fiori a destra.
Quindi leftship uno, left shift uno.
Per le industrie.
Di questo poi faccio una permutazione.
E attendo 48 B.
Ovviamente la rimontazione non solo, come dire cambia di posizione, ma poi non faccio passare tutto. Solo 48 del prodotto, della reputazione.
E questo vi garantisce che l'aspetto importante le sottochiavi siano sempre differenti, leggermente differenti però per effetto della dell'efter shift che io vado ad applicarlo.
Decifrare, stesso algoritmo, ordine inverso di chiave.
Ovviamente anche la schedulazione di chiave è uguale.
Quindi quella funzione non è solo la funzione a sinistra che diventa uguale, ma anche la funzione a destra. Quindi in realtà una sola implementazione del destro devo solo cambiare l'ordine di proposizione.
Alcune volte.
La schedulazione della chiave pre computa tutte le sottochiavi poi le fornisce in base all'operazione che voglio fare.
E dura un'ottima memoria, un po' più importante, cioè devo fare 16.
E devo memorizzare 16 elementi di 48 bit.
E ovviamente questa sua natura di avere un unico circuito è quello che ha reso il des particolarmente vantaggioso anche per l'implementazione.
Che effetto valanga che dicevo, è stato studiato da Shannon, è stato teorizzato da Shannon, ed è una proprietà che noi vogliamo dare. Quindi modificando un solo bit del testo in chiaro o della chiave o una grande modifica sul testo cifrato.
E ovviamente questa modifica non deve avere una relazione. L'ideale quindi deve essere imprevedibile. Quello che è l'effetto di questa variazione o sul testo in chiaro sulla cifrata per il des, cambiando un bit nel fraintex metà dei bit decifrato cambiano.
In cambiando un bit della chiave, anche in questo caso non siamo a metà, siamo quasi alla metà e bit non cambierà, quindi è un effetto che effettivamente civico ci piace.
C'è una caratteristica del che viene chiamato proprietà del complemento.
E quindi Lega il comportamento decifrato all'operazione di complemento, che l'inversione, quindi dove c'è zero metto uno, dove c'è uno metto zero e vale la relazione dove?
Il cifrato.
Scappa luce y.
Se io faccio il cifrato del complemento di XK, ho il complemento in Y.
E in questa proprietà non è, come dire, una fenomeno che contribuire. La sicurezza del des però in realtà taglia dimezza il numero di combinazioni che io effettivamente devo provare.
Perché ovviamente se non funziona.
Tentativo con K.
Funziona neanche il tentativo il suo complementare e quindi mi riduce.
Le soluzioni che io devo andare desclorate.
Domanda, ma se il blocco più piccolo dei 64 che faccio?
Un dato più piccolo?
Rifaccio.
Aspetto mi arrivano altri dati riempio no c'ho degli schemi. Vengono chiamati di padding, soprattutto quando era negli anni 70. Mi hai detto c'era tutte queste informazioni da cifra e

quindi potevo avere gli schemi di pudding per portare il dato a 64 3 schemi principali. Faccio due gli zeri, quindi nelle posizioni dove mancano delle informazioni ci metto lo zero.
Oppure standard ISO 3816 metto gli uno?
Quindi aggiungo uno seguito dagli zeri fino ad arrivare al 64.
Oppure IKCS5 aggiungo n byte quanto il numero di di byte di Budding.
Voglio fare tre pagine di pagine 0300303.
Problema opposto.
C'ho più dati.
Quindi non ho 64 ma ho multipli di 64.
Oppure non multipli di 64 ma riesco a riempire blog uno blocco due, blocco tre blocco quattro lo compro 11.
Il blocco fa altro bacio, va bene, o lo applico all'ultimo o spalmo il panico rispetto ai blocchi.
Però l'altro problema.
C'ho più blocchi da cifrare tutti relativi allo stesso messaggio, allo stesso dato e faccio devo usare quelle vengono chiamate in modalità operative del telefono?
La prima modalità operativa ci vogliamo, è quella facile e ci qui.
Blocco uno, blocco due, blocco tre destra ciclo, blocco uno.
Il blocco prima cifrato il cifra il blocco due usando ovviamente la nostra è una cosa uscita.
Quindi è una successione quello che lei diceva, parallelismo?
L'hardware.
Questa modalità è molto semplice.
È insicuro per quei dati che sono procedurati, perché in realtà.
Non c'è dipendenza fra i blocchi.
Ovvero prendete questa immagine e faccio la cifratura in CB invece che ha blocchi uguali corrisponde cifrato uguale.
E quindi io riesco ancora a vedere un po' l'idea dell'immagine.
Non c'è una vera e propria rottura dei legami all'interno del dato strutturato.
Per le per le mie immagini sono nel caso di struttura.
Sì, ho cifrato, ma io pinguino vedo ancora.
Quindi non è propriamente buona come soluzione.
OK.
Voglio qualcosa che mi rompa.
Queste dipendenze che se pure il mio dato strutturato è fatto da blocchi uguali non ottengo cifrati uguali, allora uso un'altra modalità che è il CBC, quindi cyber blockchaining.
Rompo il parallelismo e faccio un chaining, una sequenzialità nella produzione dei cifra e come faccio fondamentalmente il des quando cifra non riceve il blocco che deve cifrare ma riceve lo csore blocco corrente e del blocco del come dire dell'elaborazione precedente?
Game cyber blocco precedente.
Ovviamente nel round zero io non ce l'ho il precedente, quindi mi faccio dare un dato di inizializzazione della catena.
Richiamato vettore di Inizializzazione IV, che può essere pubblico.
Riuniti in noto oppure.
Lo vado a scegliere, io me lo tengo e me lo prendo nascosto.
È un cifrario ovviamente meno performante, perché è meno performante, non è caratterizzabile.
Ogni operazione attende la precedente, poi in realtà c'è anche un problema, se io cito.
Mando il messaggio a lui che deve decifrare, lui deve conoscere l'ipilo applicato.
Che ovviamente l'università ha le operazioni inverse.

Facendo le operazioni inglese, però, andranno in via.
Se io gli do un IB sbagliato o lui ha ricevuto un IB sbagliato, dal momento in tutte le elaborazioni dipendono dalla prima se la prima è sbagliata.
Lui in cascata sbaglia tutto, quindi c'ho propagazione.
Ovviamente delle verdure, però il fatto che tutti dipendono tra di loro non rendo possibile gli attacchi di sostituzione.
Devo però correggere questo problema di questo IP sbagliato che si propaga e quindi posso usare la modalità che CFB?
Dove c'ho il cyber feedback? Quindi CFB come funziona? C'ho il des.
Non vado a cifrare il blocco.
Vado a cifrare l'inizialization getto o la chiave, il prodotto in x or o il blocco da cifra.
Questo c'ha due vantaggi, il primo vantaggio?
E che fondamentalmente, i blocchi cifrati sono sempre in concessione.
Però non è detto che X con i.
Sia 64 bit.
Perché non è detto che sia senza 64 bit, perché non è il vero input del de S.
Quindi realizzo un cifrario che è un flusso auto sincronizzante.
Quindi in realtà sto trasformando il des da una cifratura a blocco, una cifratura di flusso.
Finché mi potrebbe anche piacere.
CFB però non corregge il difetto del CBC, ovvero.
Gli errori ci sta.
E se quello è sbagliato, quando decifro si propaga tutto l'errore?
Però mi realizza un flusso continuo.
Che trasforma quindi tutto in maniera interessante.
C'ho anche un'altra modalità del cfb che è il jbit, ovvero meno vit.
Ne ho solo JE, quindi che posso fare, posso scegliere?
Una quantità compresa in un registro tra uno e 64 e fondamentalmente il des riceve il cifrato riempiendo il registro.
E vado a cifrare il registro con quella chiave, poi faccio l Xorn con l'ingenti del test in chiave.
Questo fa sì che il testo in chiaro sia meno di quello effettivamente disponibile per per il test e quindi il risultato diventa ancora un flusso di titoli. Bene generali, quindi è una costruzione giusta.
No, J può essere di quinto giorno sulla legge. Non è un parametro dimensionale, è come io vado a riempire.
Mi stampo, dico possibile?
Posso avere anche un'altra modalità e l'o FPI che genera la.
Attualmente sono a partire da un inizialization Vector, però ovviamente.
La sequenza che io do al des per poter cifrare è indipendente dal messaggio perché parte dal Z0EVE, poi in realtà il cifrato ottengo l'inps ore tra il prodotto del des e il messaggio da cifrare.
Quando vedete un x olio questa maniera è sempre un centrale Office.
EZ Mony è il la confuso pseudo random che sta costruendo il centrale unico.
Parlante 4 01:02:15
Vabbè.
Parlante 2 01:02:15
Anche.
Varie costruzioni.
La parte debole della destra è che noi usiamo 56 effettivi.

Un protezione?
Finché, ovviamente, man mano che l'informatica è andata avanti.
No, non era quello. Sfoglio computazionale per mantenere il descrittore blocco.
Quindi che cosa è successo?
Blocco è piccolo.
Sono pochi i tentativi, come riusciamo ai robusti del desktop? E ovviamente il des è stato in giro per una ventina d'anni.
Quindi che avrebbe dovuto pensarne uno nuovo, si è pensato a dire, io ce l'ho.
Proposto e loguestire. Un modo può essere fare delle cifrature multiple, cioè non applico il destro una volta con una chiave, lo applico due volte con due chiavi diverse.
Quindi l'idea è stato questo doppio test dove il testo cifrato la cifratura rispetto a una chiave.
Ecco, rispetto a un'altra chiave del testo in chiaro, quanto il robusti esce il test.
O meglio, se io uso due chiavi da 56 cifrando due volte sono andato a migliorare il livello di ripetizione o rimango sempre con lo stesso livello di prevenzione?
In realtà questa costruzione vulnerabile dà un attacco e si chiama meeting Beatles. Perché meeting mea? Perché in realtà per poter rompere il test io devo fare tutti i possibili tentativi.
Per indovinare con uno.
Quanti sono uguale a 56?
Ehi.
Il fatto che Cipro due volte.
Non è detto che io devo indovinare contemporaneamente, ma posso fare un incontro nel mese.
O meglio.
Trovo le possibili combinazioni.
Per identificare K con i che mi dà una Z che io noto.
Qual è questa Z, quella che me l'ha voluta dall'altro lato?
Quindi io devo trovare quelle combinazioni.
Tali che mi trovo lo ZM.
E corrisponde a tutti e due.
Quindi in realtà non è che io sto espandendo.
Le possibilità?
Sto anche riducendo, Eh?
Perché poi mi mi fermo nel metro, quando trovo questa corrispondenza ho trovato carta comune. OK comunque.
Noto, 10.
Quindi in realtà il doppio des.
Migliorare la situazione?
Proprio per esempio di questo Stato.
E quindi che faccio?
3 M. Due.
Andiamo a non deve essere investito.
Tre volte in testa.
Con tre chiavi o con due chiavi o 303 chiavi?
Il triplo deluxe.
Ha due opzioni, quindi chiave uno, chiave due, chiave uno, quindi due chiavi chiave uno, chiave due, chiave tre. Ma l'idea è che eseguo tre volte il test.
Il triplo adesso, ovviamente.
Possibile applicare mettendo middle?

Però il fatto che io sto cifrando tre volte questo meeting middle non è tanto vantaggioso, o meglio mi trovo nel mezzo la con cui ho capito.
Mi trovo di mi trovo in quest'altro mezzo, il K1K82, quindi il totale dei tentativi è due elevato a 112.
Quindi in realtà a fronte di tre volte 56 bit.
Che fa?
168. Il livello di sicurezza è quello che otterrei con un cifrario con una chiave a 112, quindi il triplo test migliora un po' la situazione però c'ha due svantaggi, una chiave molto lunga a livello di protezione, non adeguato per quella chiave.
Spreco risorse perché ciò? Il destro che faccio tre volte, tre volte vuol dire tre volte il tempo.
E quindi triplo testi. In realtà è stato usato come funzione ponte.
Fintanto che trovava veramente un centrale migliore del terzo e il cifrario migliore dell'est, è arrivato ed è AS.
Che Advanced Encryption Encryption standard, quindi la.
Di idee è andato avanti nel pro per marcare.
Funziona su blocchi più grandi.
128.
E ha tre ordini di grandezza della chiave, 128192257, perché tre lunghezze di chiave?
Mettiti quindi la chiavetta.
Certo, però se la chiave è troppo lunga che cosa succede?
Più cicli se vi ricordate la lunghezza della chiave.
È un elemento di sicurezza.
Ma in base a quanto è lunga la chiave? C'è oggi una successione di round, troppi round, troppo tempo. Quindi in realtà la lunghezza della chiave diventa un trade off tra sicurezza e performance. La chiave a 128 sono le migliori performance. Perché la chiave?
Breve.
La chiave più lunga, due e 56, è il livello massimo di sicurezza, ma il livello massimo anche di ritardo che noi abbiamo nelle operazioni.
Okay.
Non è una rete di feste, ma è un'altra rete che è la rete di sostituzione delle votazioni che.
Atti delle operazioni semplici nella rete, ma sono operazioni non lineate con maggiore grado.
E anche una efficienza maggiore su hardware e software.
Il test in hardware funzionava molto bene, il software si arracca un po' di più.
Quindi la rete a sostituzione per mutazione SPN è una struttura che vedete qui.
Non è come feste in cui io lavoro su una parte del blog e non sull'altra, qui lavoriamo su tutte le parti.
Ed è composto fondamentalmente da una fase di confusione che le S box.
La fase di permutazione, che quindi è diffusione e poi un'operazione di xologo la chiave dichiarazione o primo o dopo queste operazioni.
Ci siete brutto?
Lo so.
Confermo.
Quinto.
Una la sicurezza e l'invertibilità deriva dal fatto che ogni pasto è matematicamente invertibile.
Attenzione, ogni passo è matematicamente inverti pubbliche. Per esempio noi negoziamo devono essere investiti, cosa che investe. Noi avevamo la F ma la che non essere divertibile e al fatto che io non lavoravo su tutti i dati.

Ovviamente festel è un po' più flessibile nella progettazione, proprio perché ha una investibilità intrinseca indipendente dall'interazione.
Invece la SPN tendono ad avere delle implementazioni più ottimizzate sul parallelismo perché se vedete tutti lavorano.
Io lavoro sempre sul blog e faccio tutte le operazioni su quel blocco e naturalmente parallelo.
Perché io posso tagliare questi pezzi ed eseguirli tutti in parallelo?
Non come dire, uno dipende dall'altro e quindi ho un forte parallelismo.
Più operazioni di esecuzione, più di più veloce rispetto.
Alla un'implementazione di feste e le trasformazioni ovviamente non distruggono le informazioni, ma le riordini mescolano così che dopo una serie di interazioni ovviamente decifrato, non ho la dipendenza contro il presso Ignazio.
Il il Cifrario AS è sempre una successione di ripetizioni.
E se vedete qua è lo schema, prendo il testo in chiaro, 128. Ho una trasformazione prima dei round n round in base alle chiavi, 10 round, 128 12 round.
192 e 14 round +2 156. Insomma, c'è una bella non mi ricordo mai niente, però di ricordare che.
Come si lavora però con AS? In realtà il blocco non lo dovete vedere con una successione di bit, ma come una matrice.
Quattro per quattro.
E si lavora sui pezzi quattro per quattro come operazioni in un.
Un GF due alla oggi, proprio in un campo di galua.
Tutte le operazioni sono ricevute via operazioni.
Anche la la chiave ha una rappresentazione matriciale.
Indipendentemente dalla lunghezza ed è suddiviso in quattro righe per NK Colonne, dove le colonne sono lunghezze della chiave di strumento.
I primi quattro byte del blocco.
Vanno a riempire il primo elemento.
Il secondo il secondo elemento lungo la colonna, quindi il riempimento segue la colonna.
Quindi quando mi arriva la successione di io riempio le colonne e poi passo la colonna successiva.
Ovviamente quando io devo fare l'operazione duale, quindi dalla matrice organizzata, devo dare il risultato io ritorno sempre andando sulle colonne.
Ok, il cuore dell'algoritmo è. Sono quattro operazioni che si ripetono.
La prima operazione è una sostituzione, quindi un sub bytes Ice and box, poi abbiamo uno shift delle righe, poi abbiamo una sostituzione delle colonne e poi abbiamo l'aggiunta della chiave.
Questo viene ripetuto 101214 volte.
Però ovviamente la trasformazione pre round.
La trasformazione iniziale non fa tutte le operazioni, ne fa solo due.
Quindi albera anche e mix forum sono realizzate su, la parte di sotto è leggermente.
Parlante 16 01:13:22
Diversa manca lo shable mobile.
Parlante 2 01:13:27
Queste sono le operazioni avvengono la sostituzione c'ho la S box corrispondente da una parte e dall'altra. La logica è sempre quella che abbiamo visto. L'elemento che devo sostituire lo uso per identificare righe e colonne della S box. Il contenuto è quello che sostituisce.

Lo chief è uno shift a destra, quella di prima riga una posizione se quella riga sempre +2 posizioni, terza riga riposizione poi la riga.
Così ci sta in maniera crescente sulle righe.
Mix forum, vado a fare le sostituzioni sui Dante delle due colonne e quindi vado AA identificare se con zero CE vado a fare una moltiplicazione con una matrice per ottenere la sostituzione derivante.
E poi infine devi fare elaborare un c, quindi faccio un insore disabit tra il blocco organizzato in matrice, la round key organizzata in matrice.
Per matrice.
Il blog 128, indipendentemente dalla lunghezza della chiave, la rauti è 128.
Ok, questo l'abbiamo visto.
Generazione delle sottochiavi, segue un algoritmo strutturato di espansione della chiave, di applicazione di rotazione di S box e costanti di round. Ogni round ha una diversa costante, che viene sommata più in generale la la chiave.
Per la decifratura ovviamente non ho le caratteristiche proprie nella rete di feste perché alcune operazioni le devo usare. La versione investita?
Quindi non posso usare le.
Parlante 8 01:15:16
Fruizioni di.
Parlante 2 01:15:18
Questo come sono, devo andare a fare quindi per tre operazioni che sono la sostituzione dei byte, quindi la S bonus per lo shift raw e per.
Un mix forum ci ho, la controparte invertita che devo andare a incrementare, devo andare ad utilizzare?
E quindi vabbè, in versione c'ho l'ICE Box inversa.
Quindi dall'elemento FUCIFRATO punto alla tabella per ottenere elemento originario. Non hai detto che quella Xbox sia la stessa dell'altra?
Shift, devo fare shift non a destra ma a sinistra, quindi l'inversione dello shift a destra e lo shift a sinistra, quindi come ho fatto di una funzione prima riga potrei fare via discorrendo?
E poi mix col comunciò, un'altra matrice delle difficoltà indietro dietro.
Quindi ovviamente sulla decifratura devo implementare alcune diverse.
Parlante 17 01:16:15
Discipline rispetto ad essere.
Parlante 2 01:16:18
Un piccolo cambiamento nel testo è chiaro, che produce un grande cambiamento. Se vedete, ecco, questo lo vedete quando ci ci abbiamo un testo zero data una chiave fair play è tutto zero. Avrò un sifer se aggiungo un vita altro alla fine guardate quanto cambia il sifer per applicazione, in quella maniera cambia fortemente. Questo è l'effetto alla valanga.
As al momento è quello che noi utilizziamo dappertutto.
Anzi, tutti i protocolli che hanno la revisione aggiornata hanno al momento AS.
No, qua in Italia.
Come chiave dipende un po' dalle esigenze di protezione.
Parlante 18 01:17:08
Il senso ci sono delle.
Cioè per far eccitare il progetto di un determinato hardware.
Giusto, e lo facciamo noi ad 8.
Potessi e abbiamo messo delle informazioni su un dispositivo.
Parlante 3 01:17:28

Dispositivo OK.
Parlante 18 01:17:30
Nuovo quel dispositivo non è più l'esempio, si usa des.
Vulnerabile, giusto?
Parlante 2 01:17:38
Devo creare un nuovo pezzo di albero ed è costoso veramente.
Comprato questo uso?
Qual è la foto citazione di un hardware canale o quattro?
Parlante 18 01:17:52
Mila euro per avere due pezzi e.
Quindi due di numeri? Sì, sì, vogliono proteggere dei dati importanti su un'antica. Anche lì bisognerebbe aggiornarli in continuazione perché ci daranno i.
Parlante 2 01:18:00
Cambi, l'albero è un po'.
Parlante 18 01:18:02
Difficile, no? Dico in generale nel se vogliono.
Parlante 2 01:18:06
Proteggere tanti vabbè, però la evoluzione dei centrali non.
È che se sono iscritti.
Normale poi il.
Parlante 18 01:18:18
Nucleo destro nell'età.
Anteriore di.
Parlante 2 01:18:22
Traduzione del dato poco e.
Poi a est.
C'è una di nipote e devi fare un aggiornamento hard del dottor di amico che saraceno, quanto costa farlo?
Quanto costa sostituire la persona?
Non è quantificabile, cioè io ti so dire quanto costa realizzare un hardware si.
Parlante 4 01:18:44
Dovrebbero essere in.
Parlante 18 01:18:45
Giro in altri articoli di test.
Parlante 2 01:18:49
Interessava non i dati, infatti progetti nell'altro era obsoleto che c'è ancora il computer.
Febbraio, un esempio di di vetro che realizza gli alberi.
Sintetizzarmi il componente.
Tradurre un concetto sbagliato, no?
Maledetto.
Ma non deve riportare nei sistema scientifici di gatti che.
Quindi io chiedo a farmi queste operazioni, poi c'è l'ingegnere del giorno, queste operazioni possiamo salvare.
Mette tutto sul gip, sto cercando di tutto. Il locale di Operazione ti dico. E poi in generale il lo schema, la scheda va in un'azienda commercializzata.
Parlante 18 01:19:47
Ora avete qui, si sta parlando un po' qua.
Parlante 2 01:20:04

Inizio, inizio, già inizio.
Parlante 9 01:20:06
Adesso fino al 2030 possiamo usare.
Verso dello sguardo dopo il 2030 non si dovrà dare più commenti.
Parlante 2 01:20:13
Sì, però ovviamente quello sta dicendo in quei settori che sono particolarmente critici nel militare, ma cioè, se io ho un mio impianto militare, il centrale è noto essere vulnerabile, non ho vulnerato.
Altri contesti magari che sono ancora più lenti o non sono critici.
Di sicurezza e adeguata possibile?
Però c'è sempre la ribourne buon consumato posto no? Se io per gestire quel rischio?
Dalle sedi 25.
Però se io produco nuovo hardware.
I tuoi nuovi cellulari, metterci le luci fra le orecchie, metterlo?
E questo poi genera.
Viaggio in un'altra volta all'altro.
Tutto chiaro?
Di affamati.
Molto.
Ci vediamo lunedì alle 9.
Parlante 18 01:21:57
1945.