Parlante 1 00:00:01
Tradizione di lunedì.
Digerita.
Parlante 2 00:00:08
C'è qualche aspetto che ancora un.
Vuol dire chiaro?
Se ci avete fatto caso ho aggiornato le slide che avevo.
Ho caricato sul team.
E oggi, intorno alla fine, un mila.
Una sorta di visualizzazione della prova che io avevo fornito a lezione. Facciamo un attimo, un riepilogo, di cosa abbiamo parlato la volta scorsa, la volta scorsa?
Il nostro obiettivo era l'obiettivo principale, quello di riuscire a dimostrare che la mozione di gruppo Obbligazionale che abbiamo espresso in termini di indistiguibilità e in termini semantici è raggiungibile, quindi questo era l'obiettivo di fondo. Vi volevo proporre un certo sistema che è in grado di raggiungere quella risoluzione per farlo.
Che cosa ho fatto?
Un concetto fondamentale che è quello di generatore pseudo casuale. Abbiamo visto quali proprietà deve soddisfare. Fondamentalmente un generatore pseudo casuale non è altro di un algoritmo detersivistico che prende pochi bit totalmente casuali, quello che chiamiamo seme e lo estende in una stringa diciamo di lunghezza arbitraria, sempre polinomiale.
Della lunghezza del seme.
Che sia indistinguibile da una stringa scelta uniformemente a caso dall'insieme delle possibili stringhe della stessa lunghezza. E quello che abbiamo cercato di capire è come definire questa immissibilità. Se vi ricordate, l'abbiamo fatto dicendo che qualsiasi algoritmo efficiente che prova a capire data un'istanza.
Gli stringa generata dal generatore ho scelto il formamento del casco, deve se deve cercare di capire da quale delle due sorgenti viene fuori, non riesce a farlo, con la probabilità fondamentalmente migliore che lanciamo una modifica, quindi il mezzo più qualcosa di trascurabile significa questo. Dopodiché che cosa abbiamo fatto?
Parlante 3 00:02:13
Ho passato un po' di tempo.
Parlante 2 00:02:18
Nell'astrarre quella che è la tecnica con la quale mostreremo i nostri risultati.
In qualche modo ho cercato di convincervi che era la tecnica che avevamo già usato nei primi due esempi di dimostrazione della lezione precedente. È fondamentalmente le cose che ho fatto ieri. Ho detto, ragazzi, di solito le le dimostrazioni saranno di questo tipo. Noi diremo se questa assunzione è vera, allora la costruzione è sicura.
Nel nostro caso particolare, quello che vi ho fatto vedere è se.
GPRG, allora lo schema legislatura chiave simmetrico del messaggio di lunghezza fissa è, è a di sicuro.
Giusto.
E come si provano queste affermazioni? Si provano ragionando per assurdo e dicendo, supponiamo che non sia vero, quindi nego il teorema. Supponiamo che non sia vero, non è vero. Che cosa significa che la costruzione non è simile?
Che significa che non è sicuro, esiste un avversario efficiente e in grado di rompere lo schermo, giusto?
Allora se esistesse questo avversario io ne potrei costruire un'altro che, servendosi di questo come sabrukin, è in grado di risolvere il problema che ritenevo difficile o di rompere la

costruzione di base che è utilizzata come diciamo black box o come blocco costitutivo all'interno della costruzione più complessa.
Ma poiché assumo che questa costruzione di base è sicura o che il problema sia difficile, questo secondo algoritmo non può esistere. E il cuore di questo secondo algoritmo che cos'è? È il supposto algoritmo contro lo schema di partenza, quindi è quello che non può esistere. Ma se quello non può esistere, allora vuol dire che la costruzione è sicura.
Questo è quello che.
Fondamentalmente abbiamo.
L'abbiamo fatto nella.
Questo salta, no?
Attimo.
Che quello che abbiamo fatto la volta scorsa spero che abbiate vi siate convinti. Diciamo di tutte le cose che ho cercato di di spiegarvi. Quindi questa era l'istanza generale.
Il teorema che piogge invece mostrato, quindi, è che questa costruzione è una costruzione struttura. Graficamente l'abbiamo rappresentata in questo modo e.
L'algoritmo che sfrutta il supposto avversario per rompere lo schema abbiamo chiamato distinguere perché il problema specifico che stavamo analizzando era il problema di capire se il generatore g è effettivamente uno pseudo casuale.
Cioè se la stringa.
Che viene pronta.
Nell'esperimento del nastrino pseudo casuale o, il nastrino oppure.
La dimostrazione, se avete fatto lo sguardo alle slide, a gennate.
E spero che si, spero che si tenga. Fondamentalmente la possiamo vedere in questo modo, quindi il teorema dice, se g è un DRG, allora la costruzione è sicura.
Prova.
Leggo il teorema e dico.
Esiste un avversario efficiente che rompe lo schema con una probabilità di un certo tipo.
Allora che cosa posso fare? Ovviamente questo è questo è uno schema della.
Parlante 3 00:05:48
Dimostrazione a.
Parlante 2 00:05:49
Siquitel'avversariocheesistecheiosupponggononpaloschermovihofattovederecomepossocostruireinvecedp.pt, che rompe il generatore.
Li prende in inbook la stringa Omega, quindi li sta giocando nell'esperimento della distinguibilità per quanto riguarda il generatore, vi ricordate? Abbiamo definito il generatore con le due proprietà. La seconda è la pseudo.
D deve cioè esprimersi e deve dire se questo Omega è pseudo casuale o è casuale. Questo è l'autobus, diciamo della T rappresentato in una scala.
A questo punto di che cosa fa? Se avete rivisto la prova, fa la cosa seguente, manda in esecuzione a, quindi sta utilizzando a come subway.
A.
Ad un certo punto.
Ha sta pensando di giocare nell'esperimento prima di K perché ha progettato per compiere lo schema di cifratura, quindi ha a un certo punto darà m zero ed M uno in output.
Immaginando che dall'altra parte c'è il challenger, quindi dicendo, questi sono i messaggi sui quali voglio essere sfidato, il distinguere sceglie il beep casuale.
Che dice cifra m zero, cifra M uno e costruisce guardate la cifra dura immergendo quella dell'istanza del suo problema.

Quindi sta cifrando n di B con Omega Dando questo cifrato ad a.
Pa restituirà?
Un bit.
Che rappresenta quella che è la sua scommessa.
Secondo me hai cifrato m zero. Secondo me hai cifrato è meglio. A questo punto i distinguo ce n'è.
Confronta di primo con il diritto.
Con PDV rappresenta quella che è la sua scelta di cifratura. Quindi se due bit sono uguali, di che cosa pensa? L'avversario ce l'ha fatta perché ce l'ha fatta? Perché il cifrato che gli ho mandato è un cifrato costruito esattamente come ricostruisce lo schema di cifratura, cioè Omega. È una stringa pseudo casuale. Perché? Perché io so che l'avversario ha successo. Nel rompere lo schema quando le cifrature sono.
Costruite col generatore questa cosa sua e quella in alto punto uno di, che sta a significare convenzionalmente.
E la stringa omnia pseudo casuale.
Se invece il test fallisce, sta in output zero, che sta a significare. Secondo me la stringa è casuale perché l'avversario non è riuscito a distinguere, e io so che quando l'avversario non riesce a distinguere è perché probabilmente la ciclatura che gli ho passato non è prodotta come nello schema, ma in particolare è prodotta come webank.
D'accordo, quindi questo è l'algoritmo che io ho proposto per dimostrare che se a rompe lo scherma, allora d rompe il generatore.
Una volta che vi ho descritto il codice, quello che ho fatto è detto perfetto, cerchiamo di capire qual è allora.
La probabilità di successip.de abbiamo analizzato due casi. Ho detto se Omega riceve input è casuale questa cifra dura è come se fosse una cifratura delle guarda in parte.
E quindi la probabilità dell'avversario quando gioca nell'esperimento privi di K il gioco dell'indistinguibilità quando c'è di fronte un'asciugatura con One time pad sappiamo che vale la perfetta indistinguibilità, quindi?
Riesce ad indovinare con probabilità un mezzo.
Giusto.
D'altra parte, quando la sfingaomegapassataadepseudocasualequindiquestoomegaeg.dk per qualche K, la probabilità che d da in output punto uno, quindi che i due bit siano uguali, ovvero che a.
Riesca ad indovinare il punto è proprio appunto la probabilità che nell'esperimento vero, perché questo è l'esperimento che vista simulando.
L'avversario riesca a.
Quindi ho legato alla probabilità che B dai un turno.
Nel primo caso la probabilità che ha da in output uno quando lo schema è il One time pad e nel secondo caso la probabilità che a da uno quadro lo schema è quello reale.
Questo è il passaggio, diciamo, interessante.
Qui utilizzo un'assunzione che il mio generatore è pseudo casuale, quindi a questo punto una volta che ho legato.
Probabilità di chi da 31 in tutti e due i casi alla probabilità dell'avversario a dico un attimo, ma io ho supposto che g fosse un generatore.
Allora che cosa ho fatto? Ho costruito di che è un algoritmo PB.
Perché? Perché i pasti che fa qua dentro, credo che siate tutti convinti, sono passi di vostro Stato. L'unica cosa che pesa è questo algoritmo è altro.
Quindi se hai il PPPD per come è stato progettato il Pd.

Depp.
E se g è un generatore, queste che cosa sono? Sono proprio le due probabilità.
Che vengono nella definizione di pseudo casualità. Nella definizione di pseudo casualità io risiedo e la differenza tra queste due probabilità sia trascurabile.
Quindi se g è un generatore, posso sicuramente scrivere che la differenza tra questo e quest'altro deve essere perspirato.
D'accordo, ma dalle uguaglianze che ho stabilito questa?
Questa.
Equivale a scrivere un mezzo meno la probabilità che ha abbia successo rispetto allo schema p equivale ABO meglio che implica. Anche questi sono due che la probabilità che l'avversario riesca a rompere lo schema è trascurabilmente negli ultimi.
OK.
Incontrabilmente, Michelle.
Quindi fondamentalmente.
Questa è una dimostrazione per assurdo in cui ad un certo punto spunto l'ipotesi che gesi ha un PRG.
Quindi questo è il passaggio in cui una volta che ho legato la probabilità che DA uno ad un caso che DA uno nell'altro caso quando il suo Imu o è una stringa casuale o una stringa uno strato casuale. A questo punto mi fece un momento, ma d è efficiente?
E per ipotesi gmpr, allora se è un PRG questa differenza deve essere trascurabile e diventa poi banale tirare fuori quello che è il risultato che voglio e cioè che il mio schema deve essere semplice.
D'accordo.
È più chiaro, era chiaro già prima.
Va meglio?
Prego.
Parlante 4 00:13:17
Quanto è forte una dimostrazione dell'assunto nella Comunità, diciamo.
Parlante 2 00:13:24
Crittografia sono tutte così, per cui sono forze, sono dimensioni. Se parla con qualche matematico turista e potrà dire che le dimostrazioni costruttive sono, diciamo hanno un valore diverso rispetto a quelle e c'è una versione.
Parlante 4 00:13:40
Costruttiva di questo.
Parlante 2 00:13:40
Soprattutto per assurdo.
La maggior parte sono dei Rossi.
Sì, allora io?
Parlante 5 00:13:48
Quindi noi abbiamo un problema che partiamo, è difficile.
Ce lo chiamiamo Y sì, in questo caso, secondo lei?
Parlante 2 00:13:56
Qual è il problema?
D'ufficio.
Parlante 5 00:13:59
Comunque le indagini la fisetta.
Parlante 2 00:14:01
Quindi in questo caso.

Tutto il problema difficile sto assumendo che una costruzione di base perché il generatore è un blocco che viene utilizzato.
Parlante 5 00:14:11
Nel mio schema è considerata simile e noi durante la costruzione noi usiamo un un'istanza del problema. Difficile, esatto.
Un però se noi Francesco.
Parlante 2 00:14:23
Dov'è lo Stato del problema? Difficile in questo caso.
Allora a è l'avversario contro lo schema di cifratura, però l'istanza.
Nello schema di cifratura è questa qui.
Cioè noi gli stiamo ponendo, gli stiamo passando una cifratura di uno dei due messaggi.
E questa istanza dello schema di cifratura l'abbiamo costruita andando a prendere la stringa Omega che è l'istanza del dobbiamo un po' meno. Quindi io sto immergendo. Nell'istanza dello schema di schema disciplina l'istanza del problema difficile consentì barassi dice, guarda io da solo non riesco a risolverlo. Tu sai rompere lo schema di cifra due? Allora faccio una cosa immergo nello schema.
Questa è la parte difficile di tutte le prove nello schema di cifratura, l'istanza del mio problema, che è ovvia in modo tale che se tu rompi.
Io riesco a dedurre dalla tua risposta qualcosa che è interessata e a me in questo caso interesse capire se ovvio casuale o se o casuale.
Parlante 5 00:15:28
Se noi assumiamo che.
Riusciamo a rompere lo schema?
Lo schema, cioè, sarebbe la costruzione digitale.
Che è un'istanza del problema difficile.
Parlante 2 00:15:41
Perché al suo interno contiene un'istanza del problema di.
Parlante 5 00:15:44
Ah OK, non è equivale a dicembre, altrimenti, come se avessimo detto, noi abbiamo già.
Tutto il problema difficile.
Parlante 2 00:15:51
Appunto no. Il problema è che io parto dal presupposto che ho un problema difficile, devo risolvere il problema difficile in questo caso è diciamo è una costruzione.
Sto assumendo che sia un generatore, quindi.
Di cerca di confutare il fatto che gira un generatore.
D'accordo, e lo fa utilizzando AA, è un algoritmo che però risolve un problema diverso, cioè è in grado di rompere uno schema di cifra vita. Scegli due messaggi dal Challenger, il charge ti renderti dalla cifratura. Allora di che cosa fa? Dice, come faccio a decidere Omega se è casuale o di pseudo casuale?
Spirito dello schema di cifra dura contro cui ha la vera è dato dalla dal messaggio in ixor con una stringa pseudo casuale.
Allora io non si fa sta cosa c'ho questa sfida? Devo decidere. Provo a costruire una cifra prima.
Se la stringa di pseudo casuale c'ha proprio la forma che l'avversario riesce a rompere.
Se invece Omega non è casuale, io costruisco. La cifratura, però è qualcosa che l'avversario.
Non riconosce bene, cioè se c'è una signora casuale noi lo valutiamo. Dopo vediamo che l'avversario riesce a distinguere con probabilità esattamente un mezzo non ha nessun

vantaggio. Se però è per primo tipo, noi abbiamo supposto che a lavora bene contro quello scritto e quindi distinguo contro bandalità maggiore di mezzi. Ma allora il mio Pd?
Da uno se l'avversario distingue e da zero se non di distingue.
Andiamo a portare la probabilità che da uno.
Diciamo se la ***** è casuale e se la stringa è stato casuale, è quello che mi serve per confutare la proprietà.
Vado a fare l'analisi e viene fuori fondamentalmente.
E questa differenza se.
L'avversario rompe con una probabilità non trascurabile, è a sua volta non trascurabile.
D'accordo, se ci fate caso in modo diverso per leggere.
Non so perché salta stamattina, ma forse non c'è un'imitazione cortana?
Quello non dovrebbe saltare più quando non c'è alimentazione, quindi non è caricato e per qualche motivo strano o non c'è l'inversione dei portatili. Il.
Il proiettore va in standby.
Se ci fate caso, io ti ho detto.
Supponiamo che la probabilità con cui ha.
Diciamo rompa lo schema, rompa lo schema è YZ, alla fine questa probabilità trovi epsilon viene.
Cioè in questa assunzione io faccio vedere sfruttando l'assunzione che giro in DRG faccio vedere che questa probabilità deve essere minore o uguale di un mezzo +4.
Se invece.
Questa differenza fosse non trascurabile, fosse non trascurabile, ecco.
Questa quantità sarebbe non trascurabile.
D'accordo.
A quante persone è chiara la dimostrazione?
Allora per chi ancora c'ha qualche difficoltà, questa è la prima, poi una volta mi rendo conto che non è facilissimo perché bisogna un po' entrare nella mentalità.
Riguardate la conferma. Se avete ancora difficoltà per piacere scrivetemi e venite pure al ricevimento. Se può pensare che possa essere possa essere di aiuto, vi faccio notare giusto due cose che saranno importanti sempre affinché queste dimostrazioni funzionino. Ragazzi, l'ho scritto all'altro.
Di emula l'esperimento criticato, cioè di perseguirsi dell'avversario. A deve in qualche modo simulare gli esperimenti, esattamente come.
Si svolgerebbe l'esperimento reale perché l'avversario a è in grado di rompere lo schema nell'esperimento critico di K.
In questo caso, ragazzi, la simulazione è perfetta, l'avversario a non si accorge di nulla, perché nell'esperimento reale che cosa succede?
Scegli due messaggi e mi dà il Challenge. Il Challenge ne sceglie uno a caso, quindi lancia la monetina e se esce 0 5 m zero. Se esce 1 5 guardate che d sta facendo esattamente la stessa cosa. Sceglie DA caso in 0 1 se esce 0 5 n zero se esce uno circa in meno.
D'altra parte se omegaepseudocasualechecosasignificacheomegaeugualeag.dk per qualche K scelta uniformemente a caso, quindi questa cifra per la C è m in xog.dk, che è esattamente quello che a vedrebbe nell'esperimento reale, quando ci sta il Challenger e il Challenger costruisce la cifra due del Sud, quindi questo è l'aspetto importante.
Quando faccio queste prove l'importante è che di.
In generale l'algoritmo a primo che abbiamo chiamato riduzione.
Per sfruttare a ripreni perfettamente l'ambiente per il quale a è progettato, per intenderci, ragazzi come quando voi scrivete un programma e utilizzate una suppl di una funzione di

libretto, quando invocate la funzione di libreria dovete passare i parametri che la funzione di sospetto.
È solo in quel caso, funziona perfettamente, perché se invece passate anche non è detto che la salute si funziona.
Allo stesso modo, se AA è un algoritmo, diciamo molto sensibile all'indietro e all'ambiente, se si accorge che non sta girando nell'esperimento ma sta girando in un ambiente diverso, non è detto che l'autore sia garantito della stessa qualità di quello che produce nell'esperimento reato.
D'accordo, quindi questo è il dettaglio sempre importante, la simulazione sia fatta per te.
Allora Detto ciò, se è tutto più chiaro che volevo soltanto mettere in evidenza, volevo soltanto iniziare questo aspetto, non so se nelle slide l'avete visto.
Tutta l'analisi che noi facciamo di solito è asintoma. Quindi per ogni parametro di sicurezza otteniamo diciamo un'altra volta il parametro di sicurezza, otteniamo una garanzia che lo schema sia sicuro per quel parametro di sicurezza, quindi la probabilità vi ho detto che epsilon di n.
I tempi di esecuzione sono ripiene, però nella pratica, se abbiamo necessità, diciamo di produrre un'istanza concreta.
Ed è un valore di m specifico, cioè vogliamo fissare una chiave e vogliamo capire qual è la probabilità. E allora guardate che in tutto il ragionamento che ho fatto è molto semplice, se necessario ottenere una limitazione concreta, perché dovremmo fissare le linee e assumere che il g sia TYP pseudo casuale? Che cosa significa? Ragazzi, sto assumendo che qualsiasi.
Avversario.
Si può eseguire al più per i passi.
Riesca a distinguere un'assegno pseudo casuale prodotta dalle generatore da un'assegno totalmente casuale con probabilità al due.
Quindi questo significa vi ricordate quando?
Ora.
Posso per esempio fissare chi ha due lontano ed epsilon a due alla -60.
Possiamo far vedere quindi, usando esattamente la stessa dimostrazione, gli stessi passi che il nostro schema di cifratura che fa solo col PAD cellula attuale, risulta T meno c epsilon sicuro.
E come facciamo, ragazzi? Molto semplice.
Dobbiamo semplicemente qui stiamo dicendo che il generatore partiamo dal fatto che supporta avversari fino a Atti bassi.
Dato qui sto dicendo che lo schema che costruisce.
Usando il generatore supporta avversari che hanno una potenza simile ma leggermente più bassa, t, meno c.
Come faccio a provare questo risultato?
I ragazzi lo faccio esattamente con la stessa conversazione che ho fatto prima.
Questo di.
E alla fine lo possiamo vedere in qualche modo come.
Un avversario che tratta il generatore e quindi quando dico che questa differenza deve essere trascurabile nel caso concreto sto richiedendo che questa differenza deve essere minore di AY per ogni d esegue al più per più basso.
Giusto quindi se io faccio la stessa prova con valori concreti?
Ma allora?

L'avversario viva. Che cosa è costruito? Da un punto di vista del calcolo è costruito da i passi che esegue hahaha più altri passi che effettua lui, cioè lancia la monetina, fa un ixorder.
Posso calcolare questo tempo complessivamente come un tempo costante in questo caso, perché sono nuovi passaggi.
Posso chiamare questo tempo C allora il tempo di esecuzione che di da che cosa è la è dato da C?
Più il tempo di altro.
Se consideroachehannotempofinoattiverocciniquindituttigliavversarichehannotempofino.at meno CE vado a fare la somma, ottengo un avversario B che AA più.
Tempo di esecuzione attivo.
Giusto.
E quindi?
Se io sono partito dall'assunzione che il mio generatore iepsilon sicuro?
Questa prova che ho.
Vale per tutti gli avversari, hanno tempo al più i vaccini.
Vi trovate?
E naturalmente questo modo di ragionare.
Lo posso applicare?
Essenzialmente ad ogni risultato asintotico che vi do una volta che abbiamo trovato una riduzione.
Della sicurezza della nostra Costituzione.
Quella che è la primitiva andando a fissare, diciamo, dei parametri di sicurezza per la Primitiva possiamo dedurre delle garanzie concrete alla sicurezza effettiva della nostra.
La costruzione offre.
In relazione ai parametri della primitiva di partenza.
A me.
Parlante 4 00:26:33
È chiaro che due all'ottanta è un numero enorme, due alla -60 è carturabile, ma qual è il confine?
Diciamo chi le ha stabilite queste costanti, la potenza?
Parlante 2 00:26:44
Computazionale, di cui.
Disponiamo al momento OK, le faccio un esempio, fino a un po' di tempo fa per esempio.
Anni fa anche due alla 62 alla 64265 erano considerati valori ragionevoli, poi a un certo punto proprio attaccando una funzione di hashing sha.
Due alla 60 passi sono stati realizzati o alla 61 non mi ricordo esattamente, quindi quel numero di passi è diventato qualcosa che è raggiungibile.
Quindi diciamo che pian piano che la.
Partenza con il nazionale aumenta e quindi si.
Si riesce ad alzare il numero di passi che un avversario riesce a fare in tempo ragionevole.
Nell'analisi concreta si vanno a fissare i valori, diciamo che ci garantiscono sicurezza. Quindi al momento fare una ricerca nello spazio in due alla 80 elementi ancora qualcosa per non è fattibile con l'altro.
Potenze dovutazionali riguardiamo, però la risposta alla sua domanda è, è l'analisi concreta degli algoritmi, dell'efficienza degli algoritmi di cui disponiamo e della potenza di classe sublispondente.
Parlante 4 00:27:51

Per quanto riguarda la probabilità, invece?
Parlante 2 00:27:55
La probabilità questa è un po' più difficile.
Quindi è una garanzia che ci.
Parlante 4 00:28:04
Il due alla 60-1 non è più, cioè già è non è non trascurabile.
Che significa 2^2 alla 60-1?
Parlante 2 00:28:15
E qual è il cioè allora il confine è che in lui, nella teoria stabiliamo e noi ci preoccupiamo delle probabilità che sono trascurabili e l'abbiamo in effetti con la classe di funzioni trascurabili.
Quindi per noi che sviluppiamo la teoria, le proprietà di cui non ci interessiamo solo le probabilità e sono appese. La funzione se si ricorda e vanno quindi è una Convenzione che stabiliamo noi potremmo sviluppare diciamo in maniera diversa, anche una teoria, andando a considerare per esempio le funzioni trascurabili, quelle che decrescono meno di unesponenziale.
O di uno su un esponenziale. Potremmo fare allo stesso modo, però, per le ragioni di cui vi ho parlato, tipo la composizione di coloro i nomi dei proprietari di cui godono, la somma dei conti di trascurabile eccetera eccetera, la scelta che è stata fatta è qui.
Chiaro a tutti quello che sto.
Ragazzi, altri dubbi?
Perché se siete convinti?
Su questa diciamo su queste cose.
Ci volevo tornare perché mi sono reso conto che la volta scorsa qualche dubbio era era rimasto, spero che sia tutto più chiaro.
Non vi scoraggiate se avete ancora dubbi, non vi scoraggiate perché sono le prime elezioni, sono quelle più astratte, sono quelle in cui stiamo cercando di entrare in questo linguaggio per cui.
Leggete, rileggete, cercate di capire se avete lui.
Contattare, noi cerchiamo di risolverli assieme.
Quello che volevo.
Invece fare cominciare a fare nella nella lezione di oggi.
Diciamo che la cosa influente.
Fondamentalmente vorrei.
Fare due cose.
La prima è.
Se ci avete fatto caso, le nozioni di sicurezza che abbiamo introdotto fino ad ora per uno schema di cifratura a chiave asimmetrica considerano sempre.
Lo scenario in cui Alice poco vogliono comunicare, Alice invia un messaggio a poco, l'avversario guarda il cifrato, quindi è un avversario che ascolta, guarda il cifrato e cerca di carpire informazioni sui messaggi sottostante, quindi è una definizione che considera proprio lo scenario di base.
Però l'abbiamo detto più volte, se utilizziamo uno schema di cifratura in un'applicazione ci interesserebbe avere una definizione in cui Alice voi inviate 150 messaggi a Bob ed essere sicura che i suoi messaggi sono sicuri rispetto anche ad un avversario che li ascolta tutti i 150, cioè vogliamo la garanzia che non è che un avversario ne ascolta 100 e poi gli altri 50.
Riesce per esempio a decifrare o riesce a capire informazioni?

E allora quello che voglio fare oggi nella prima parte è introdurre formalmente le altre nozioni di sicurezza di cui, se vi ricordate, abbiamo anche parlato un po' di tempo. Fabio parlato di attacchi di tipo monflintex, cioè semplice. Quindi voglio un attimo ragionare su queste definizioni e l'altra cosa che poi voglio cominciare a farvi vedere è.
Se diamo delle nozioni, la prima cosa che dobbiamo fare è provare che siano raggiungibili e quindi dobbiamo esibire delle costruzioni. Per esibire delle costruzioni abbiamo bisogno di uno strumento che è più potente rispetto al generatore giusto, casuale ed in qualche modo lo estende.
E su ed è rappresentato dalle funzioni pseudo casuali o come caso un po' più ristretto, dalle permutazioni e pseudo casuali. Ragazzi, questo diventa veramente un concetto fondamentale per tutta la crittografia asimmetrica. Tutte le cose che anche vengono realizzate nella pratica, come vedremo, sono sono in qualche modo approssimazione di o funzioni o permutazioni pseudo casuali.
E.
Diciamo fare ciò distenderò in qualche modo anche.
Il linguaggio?
E utilizziamo nel costruire esperimenti.
Che ci permettono di fare le definizioni di sicurezza introducendo questo nuovo oggetto che chiameremo oracolo.
Quindi questo è quello che vorrei cominciare a fare oggi.
E mi fermo, quando il nostro, quando il tempo.
Si resta, insomma, sicuramente e quando il tempo non.
Parlante 1 00:32:47
Riscalda allora?
Parlante 2 00:32:49
Cominciamo dall'inizio, fino ad ora l'avversario ascolta passivamente la trasmissione ha accesso all'enciclopedia delle due parti oneste, si scambiano.
EE lì vuole cercare di garantire informazioni, sarebbe utile avere una nozione di sicurezza che permette alle parti di inviare messaggi utili.
Grazie come volendo.
Usare un esperimento, come formalizzereste voi?
Questa questa richiesta.
Allora nel giochiamo sempre consideriamo sempre la nozione di distinguibilità, perché abbiamo visto che è quella che ci permette più facilmente di lavorare. La prova che vi ho esibito della sicurezza dello schema che usa il genere, allora fosse quello casuale, USA il paradigma dell'indistinguibilità, giusto?
Allora, volendo costruire un esperimento basato sul paradigma dell'indistinguibilità in cui voglio.
Modellare la sicurezza dello schema rispetto all'invio di messaggi multipli. Poi che cosa farete? Come lo disegnereste questo esperimento?
In quello di base, l'avversario sceglie due messaggi, M zero ed m uno li dà al challenger, il challenger gli dà la cifratura di uno dei due.
OKE, in questo caso ci abbiamo scelto tra più messaggi.
Parlante 6 00:34:13
Di doverne inviare denuncia di B la scelta non sarà tra l'esempio m zero e -1, ma da M0AMON.
Parlante 2 00:34:23
E quindi che cosa farebbe l'avversario? Per esempio un po' di messaggi?

Li manda al Challenger?
Parlante 6 00:34:32
Sì, però per quello che dicevo, quella il significato devono essere di della stessa lunghezza.
Parlante 2 00:34:38
OK, giustamente come dice il vostro collega dice devono essere della stessa lunghezza, perché se li però lo dobbiamo un attimo formalizzare allora nel caso di un unico messaggio.
L'avversario che cosa fa, ne sceglie due.
Il Challenge ne cifra uno dei due è l'avversario deve scegliere. In questo gioco invece, che cosa vogliamo che l'avversario faccia? Qual è l'obiettivo poi dell'avversario?
Cioè l'avversario che fa?
Scegli due messaggi.
Ok, però questo è l'esperimento precedente.
Noi vogliamo l'esperimento che modelli il caso che l'avversario può vedere cifrati di messaggi utili, giusto?
E ancora, però non deve essere in grado di sfruttare questa cosa, per esempio per carpire informazioni sui messaggi impostati.
Allora vediamo se vi convince ragazzi il modo in cui.
È fortunato. Questo requisito è il seguente, nel nostro testo l'esperimento si chiama come prima, solo che viene aggiunto, è Azimut. Per ricordare o per stressare il fatto che stiamo continuando l'avversario, guardate da Einaudi due liste della stessa lunghezza, quindi è per zero grande m uno grande che contengono.
I messaggi e questi i messaggi, come potete vedere.
A coppia a coppia sono della stessa lunghezza.
D'accordo. Perché altrimenti se avesse una lunghezza diversa, sarebbe introducendo un elemento facile di distinguibilità d'accordo.
Cioè sarebbe un requisito più difficile da da gestire. Lo schema di cifratura dovrebbe.
Evitare che possa esserci una distinzione semplicemente sulla lunghezza, però abbiamo detto che negli esperimenti che consideriamo non ci preoccupiamo di proteggere la lunghezza e nella pratica abbiamo detto del 60 messaggi vengono venduti alla stessa lunghezza.
Il Challenger come prima sceglie un Bitcoin.
Una chiave per cifrare utilizzando l'algoritmo generazione dell'orizzonte specifico e guardate che cosa fa.
Cifra.
MDB per oggi. Cosa sto dicendo? Sto dicendo che questa volta o cifra tutti i messaggi dell'umanista o cifra tutti i messaggi della seconda lezione.
D'accordo, l'avversario questa volta riceve, quindi ti cifrati.
E come prima deve stabilire se questi riciclati corrispondono alla prima lista o corrispondono alla seconda linea.
D'accordo.
E ragazzi, tutto funziona come prima, se l'avversario.
Vince.
Allora vuol dire che fondamentalmente ha rotto lo schema se l'avversario non individua il visto.
Dato che dell'esperimento è zero, che significa che l'avversario ha fallito? E come potete immaginare, la definizione di sicurezza resta fondamentalmente la stessa con un nuovo esperimento, cioè.
Uno schema di rete che è.

E ha cifrature multiple, indistinguibili se quando andiamo a considerare il nuovo esperimento.
Qualsiasi avversario efficiente riesce a vincere con una probabilità che è intrascurabilmente migliore di un mezzo.
Quindi siamo esattamente.
Usiamo esattamente lo stesso linguaggio dei ragazzi, saremo sempre questo linguaggio, diamo un esperimento e diamo la definizione poi.
Considerando la performance dell'avversario all'interno delle degli esperimenti ragazzi, perché?
Vi dovrebbe convincere questa definizione? Vediamo se.
Parlante 6 00:38:43
Prego, quindi se l'avversario riesce a rompere lo lo schema, scopre tutti i messaggi di.
Quella lista non solo.
Anzi, non allora.
Parlante 2 00:38:52
Stiamo parlando sempre di indistinguibilità, l'obiettivo dell'avversario è semplicemente capire se.
Quella lista decifrata corrisponde alla prima vista o alla seconda, quindi.
Lo schema è rotto se l'avversario riesce semplicemente a respirare.
Perché se riesci a distinguere vuol dire che in qualche modo.
È riuscito a trovare in quell'insieme delle città in una qualche relazione che gli permette di capire che lì sotto ci sono i messaggi con la prima lista e mentre la seconda. Ricordo che l'obiettivo semantico che noi vogliamo è che il cifrato non rilascia l'avversario. Nessuna informazione aggiuntiva se lui riesce a distinguere qualche informazione aggiuntiva gliel'ha lasciata.
Niente.
Quindi rompere significa sempre questo? Beh, in base alle due liste di messaggi sono uguali o sono diverse tra di loro? L'avversario, quello che vuole sono le lunghezze, uguali a scelte.
A volte quindi sulle lunghezze non c'è nessun elemento che permette parametri, poi l'avversario può fare quello che vuoi. Magari, che ne so, può costruire nella prima lista i primi tre messaggi scelti a caso e li replica nella seconda lista.
Per esempio, però se fa una cosa del genere è un po' stupido perché in qualche modo diciamo che.
Si sta privando lui stesso di distinguere nella prima parte, però può fare quello che vuole. Si può mettere nella prima di ordine crescente utilizzato in modalità, può fare quello che vuoi.
Ripeto le strategie, non vorrei che consideriamo male.
Rispetto al caso del messaggio singolo, i messaggi potrebbero essere legati tra di loro, appunto, l'avversario li potrebbe scegliere con qualche relazione. Perché? Perché il suo scopo è quello di distinguere. Quindi dice, allora faccio una cosa, se li scelgo tutti a casa va bene. Alla fine ho delle decifrazioni, invece ci dice, mo provo a vedere se mi collego, magari i cifrati ereditano questa dipendenza e io riesco a capire.
E le stesse cicature potrebbero essere legate tra di loro e con i messaggi.
E questi legami potrebbero essere vicinamente, calcolabili e sfruttabili da un avversario.
Tenete presente che queste sono tutte informazioni che l'avversario in qualche modo è difficile. Mette riuscirebbe a dedurre se riuscisse.
5.
E allora?
Ma se l'avversario non riesce a capire se il ci con uno non C con d corrisponde alla.

Prima dice tu alla seconda lista.
Allora che cosa sto dicendo? Sto dicendo che il quadro non riguarda.
E quindi, ricordando l'equivalenza di distribuibilità semantica di cui abbiamo parlato, la che lezione fa allora lo schema di cifratura maschera meno ben contenuto in riciclaggio e dovrebbe convincerci.
D'accordo.
Benissimo.
La cosa che credo sia un tegliato a osservare, se costruisco uno schema disciplinatura.
E provo e è sicuro rispetto all'invio dei messaggi.
Ovviamente è sicuro rispetto all'invio del singolo messaggio.
Giusto, perché i ragazzi?
Parlante 7 00:42:08
È come se io stessi questo.
Parlante 2 00:42:10
Esperimento, se ci pensate, è una generalizzazione di quello che l'indistituibilità se considero liste di rivezza uno.
Sto riproducendo un esperimento.
Egli è banale, uno schema sicuro in accordo a questa definizione.
È sicuro?
Messaggi.
Purtroppo.
Non vale l'universo?
Cioè.
E se ci pensate un attimo, lo conoscete già, posso esibire uno schema che è sicuro.
Rispetto ad un unico messaggio, ma non è sicuro rispetto all'invio di quei messaggi.
E se ci pensate, lo schema che prova questa affermazione è proprio riguarda i fatti.
Per quale motivo? Il One Time Pack abbiamo dimostrato che è perfettamente segreto, ma in accordo alle.
Giusto e la perfetta indistinguibile.
La è un caso particolare, è una nozione ancora più forte rispetto alla indistinguibilità computazionale. Perché? Perché nella indistinguibilità Computazionale sto richiedendo che gli avversari sono limitati.
E l'avversario possa distinguere con probabilità al +1 mezzo più qualcosa di trascurabile nella.
Perfetto e distinguibilità, l'avversario fa potere infinito e riesce a distinguere con probabilità esattamente un mezzo.
Quindi il One Time Pack e l'ho scritto qua.
È sicuramente uno schema che soddisfa la.
Nozione di indistinguibilità per l'invio di un unico messaggio.
D'accordo, questo l'abbiamo già visto la volta scorsa.
Abbiamo detto che però non era interessante perché noi abbiamo introdotto la nozione disabilità computazionale perché volevamo produrre uno schema che ad una chiave breve.
Associa cifrati lunghezzabilità, quindi quando io vi ho dato la nozione di indistinguibilità computazionale, ho detto guardate questa nozione. Sicuramente la possiamo raggiungere con il One Time Pad, perché il One time fate supporta avversari molto più potenti e.
A un ventile più stringente sulla probabilità dico, quello che però ci interessa far vedere è che possiamo soddisfare la definizione con schede di cifratura in cui la chiave è piccola e i cifrati possono essere gravi, ed è quello che abbiamo fatto la volta scorsa.

Ora però.
Stiamo ragionando sulle nozioni del fatto e quindi sto cercando di dimostrarvi che l'indistinguibilità multipla implica l'indistinbilità singola.
L'indistinguibilità singola non implica la pubblica e per far vedere che non implica la musica basta che vi faccio vedere che esiste uno schema che.
Soddisfa l'invisibilità singola, ma nulla.
Per fare ciò sto prendendo onedrive, il One Time Pad soddisfano.
Ma non soddisfa la multipla perché vediamo un attimo se vi convince.
L'avversario che vado ora a costruire nell'esperimento che vi ho appena dato rispetto allo schema OTP?
L'avversario potrebbe fare la cosa seguente, nell'esperimento appena descritto sceglie due liste di messaggi.
Nella prima lista ci mette lo stesso messaggio zero che è implicato delle volte, quindi zero è implicato delle volte. Queste sono due stringhe di L Zero su pare quadro. Invece in M uno mette il primo messaggio uguale ad LZE, il secondo messaggio uguale ad l'uno.
Quindi l'egoismo sono differenti perché i secondi messaggi sono diversi.
Skill Challenger come al solito, che fa?
Sceglie il dp.de cifra i due messaggi.
Ragazzi che. One PIECE PAD la cifratura, come avviene? Scelta la chiave, faccio l'xbox con la chiave.
L'avversario che una volta che ha ricevuto in due cifrati vede se sono i guardi.
Dai Notebook zero che significa secondo me ha cifrato la prima lista.
Se sono invece diversi da inautocultura?
Ragazzi.
Qual è la probabilità che questo avversario indovini?
La probabilità è uno, per quale motivo?
Il One Time.
È deterministico sceglie una chiave KE.
Grande operazione VIP Searching.
Quindi che cosa succede se cifra gli elementi della prima lista?
Zero YK.
Zero XOK è esattamente lo stesso valore.
Giusto.
Se hai due messaggi sono diversi facendoli sono una chiave fissata con due messaggi diversi, ottengo due stili diversi.
Quindi fondamentalmente se V è uguale a zero.
Ovvero Challenge cifra. La prima lista ci vuole uno sicuramente uguale a. Ci conducono quindi l'avversario da zero e quindi dopo.
Se invece il beat B è uguale ad uno, quindi il challenger cifra la seconda vi.
I due messaggi sono di due cifrati, sono sicuramente diversi.
Mi trovate?
Quindi ragazzi, vuol dire che il nostro avversario.
Distinguere tutto o probabilmente a uno ha quelle probabilità più trascurabili.
Giusto.
I ragazzi quindi questo prova?
Uno schema.
Che soddisfa.
La mozione di invisibilità per un messaggio singolo.

Non soddisfa la nozione di indissolubilità per i messaggi energetiche.
Quindi sicuramente possiamo dedurre visto che abbiamo fornito il Controesempio.
E la mozione di distinguibilità per i messaggi singoli non implica il soddisfacimento da parte dello schema della nozione.
Indistinguibilità per messaggi utili.
Vi voglio far notare anche un'altra cosa.
Si riprova, la cosa che vi invito a fare è a ragionare sempre per capire qual è la proprietà essenziale che sto sfruttabile in questo caso. Guardate, io sto sfruttando il fatto che il ma in parte è deterministico, cioè scelgo una chiave. K ho ceduto, lo metti a caso? Riguarda il fatto. Però poi quando cito faccio l'X or con la chiave se devo cifrare due messaggi.
Prendo la chiave. OK, solo il primo. Prendo la stessa chiave, faccio il zoccolo secondo.
Se sostituisco, all'ixor una qualsiasi funzione.
Sempre deterministica.
Secondo voi che succede in questa fase?
Parlante 4 00:49:31
Eternistica.
Sì e non cambia nulla perché stesso input, stesso Outlook proprio per definizione.
Parlante 2 00:49:37
Di che cosa significherà? Che se uso una qualsiasi determinissima quando togli gli input zero alla l ottengo qualche cosa, quando gli do l'input zero alla l ottengo La salsa stringa.
Quando gli do due stime diverse c'hanno due cose diverse, quindi questa analisi che ho fatto qua sotto la posso rifare tale qua?
Quindi ragazzi, in realtà io continuo a usare qualcosa di più forte, con questo contro esempio ho dimostrato che.
Per qualsiasi sistema di cifratura in cui la funzione di cifratura è deterministica non posso.
Avete la sicurezza rispetto all'invio di messaggi utili?
Questi sono i risultati importantissimi.
E ho raccolto nella seconda slide, se uno schema è deterministico, la cifratura dello stesso messaggio dà sempre lo stesso cifrato, quindi la definizione.
Lì.
Cifra dura rispetto sicurezza rispetto alle più scelte multiple?
Richiede una cosa importante, richiede che.
La funzione.
È la funzione di cifratura sia probabilistica.
Ovvero, cosa significa?
Significa che devo necessariamente progettare il mio schema?
In modo tale che quando lo stesso messaggio viene cifrato più volte.
I cifrati siano diversi.
E.
Un modo per farlo? In realtà l'unico modo per farlo in accordo alla sintassi che abbiamo convenuto gli schema di cifratura è che l'algoritmo di cifratura sia probabilistico, cioè scelga bit casuale.
D'accordo, e al momento vi ripeto, poiché questa cosa forse non l'avete vista ancora, mi.
Potete avere dei dubbi.
Per esempio lo scritto nella Slide sembra un requisito questo della cifratura probabilistica che configge dell'operazione di Decifratura perché prendo un messaggio circa una volta ottenere il cielo circa un'altra volta ottengo ci vuol dire lo circa un'altra volta ottengo ciclo prego tengo stringhe diverse come fa la funzione di decifratura che è deterministica

indipendentemente dal fatto che il dolce i volumi c con due OC con tre a darmi sempre lo stesso messaggio.
Al momento intuitivamente questa cosa mi potrà sembrare estrarre, se vi sembra strano non vi preoccupate perché vedremo che invece.
Lo possiamo, lo possiamo fare forzatamente d'accordo.
Il risultato però che abbiamo ottenuto è il seguente, che se p è uno schema di cifratura con funzione di cifratura deterministica, allora lo schema non può avere cifrature multiple indistinguibili in presenza di un ascoltatore.
E questo risultato onorato?
Memorizziamo e mettiamolo avanti.
In realtà.
Quello che noi vogliamo da uno schema reciproco è qualcosa di più.
Vi ricordate i vari modelli di attacco di cui abbiamo parlato?
Il modello in cui l'avversario ascolta semplicemente.
È il modello più semplice.
Possiamo immaginare invece scenari più complessi, in particolare?
Possiamo immaginare lo scenario in cui.
L'avversario ha l'abilità di esercitare il controllo parziale su ciò che una parte onesta cifra.
Quindi, per esempio.
Possiamo immaginare il caso in cui l'avversario chieda in qualche modo, con qualche sotterfugio ad Alice di decifrare M con uno, m con due M con d.
Alice lo fa.
L'avversario che osserva poi ad un certo punto, al di là del controllo dell'avversario, ma dice cifra un messaggio con la stessa chiave per il Bob e a quel punto l'avversario può cercare di capire cosa c'è in quel messaggio o di capire informazioni su quel messaggio sfruttando la conoscenza che ha delle coppie messaggio cifrato che ha raccolto precedentemente.
Quindi.
Questo, come potete immaginare, è uno scenario di attacco molto più potente rispetto a vedere semplicemente cifrature ottime.
E.
Anche in questo caso vogliamo definire la sicurezza di uno schema in affronto alla mozione di investimenti.
Okay.
E come lo facciamo?
I primi due passi?
Nel nostro esperimento dovranno essere modellati in.
In qualche modo per poter dare all'avversario la possibilità di ottenere conti. Il messaggio cifrato.
Giusto.
L'ultimo passo, quello in cui Alice autonomamente.
Scrivi un messaggio lucifra e lo invia a POP. Lo possiamo modellare come abbiamo fatto negli esperimenti precedenti, cioè possiamo supporre che il nostro.
Avversario.
Scelga due messaggi che nella realtà corrisponde al fatto che sa che Alice, quando cifra il messaggio autonomamente, in realtà sceglie il traduttore messaggio. È un'ipotesi conforte che facciamo? L'avversario potrebbe non trovarsi in questa condizione, però se utilizziamo un'ipotesi forte, il nostro schema ci dà una garanzia di sicurezza ancora maggiore.
Quindi.

Supporremo che l'avversario.
Possa scegliere due messaggi, si passa al Challenger, il Challenger gli fornisce il cifrato C.
E l'avversario, ancora una volta, dovrà essere incapace di capire se ci corrisponde alla cifratura di e penso di meramente.
D'accordo.
Ragazzi qual è il problema al.
Momento ah, prima di tutto.
Questo tipo di attacchi.
Sono gli attacchi.
Di tipo perché sono il tipo social.
L'indirizzo per questo, data l'avversario, la possibilità di scegliere i messaggi. Se vi ricordate, quando vi ho parlato dei quattro scenari di attacco ho parlato di cyber tech, soli non flatex, cioè semplice e cioè il cybertech cybertech rivedremo fra un po' perché sono quelli più difficili da gestire. Non blinktex, in realtà non ce ne occuperemo perché sono un caso particolare.
Del Choir Planetex, in cui l'avversario per qualche motivo riesce ad avere.
Queste cuffie messaggio in chiaro corrispondente cifrato però non ha controllo sui messaggi, quindi ci occuperemo e cercheremo di raggiungere direttamente la nozione chusemplinex in cui.
L'avversario può anche scegliere i messaggi di cui vedete i cifrati. E allora la domanda che qualcuno mi può porre è, funziona a senso che ci preoccupiamo di appalti del genere? Guardate gli attacchi del genere sono all'ordine del giorno. Il vostro testo, e ripeto, vi lascio uno sguardo, cita due esempi.
Che corrispondono ad episodi storicamente accaduti in cui attacchi di lettrice o semplice sono stati fondamentali.
In particolare.
Per tentare di rompere, non so quanti di voi hanno visto. Ci sono diversi film a parte delle Imitation Game. Ce n'è anche un'altro enigma. Non ricordo il titolo in cui questi episodi.
Sono ben narrati per descrizione, in pratica per cercare di rompere lo schema di cifratura che utilizzavano i tedeschi gli inglesi durante la Seconda guerra mondiale, crescono. Questa cosa posizionarono delle linee in alcuni posti in cui le coordinate ovviamente erano note.
Dopodiché.
Cercarono di ascoltare la trasmissione dei messaggi dei tedeschi alla base in cui comunicavano che avevano individuato delle linee in alcune posizioni, ovviamente in quel caso cosa comunicavano nel Testaccio? La posizione in cui si trovava la mina e quella era un attacco di tiro. Joseph wireless perché gli inglesi avevano messo le 1000 esattamente su quella posizione.
Quindi il contenuto del messaggio lo conosceva e godevano quindi.
Dato il concetto messaggio in chiave vedere qual era il dato che veniva trasmesso dai tedeschi?
E c'è un'altro episodio storico che è sempre interessante.
Ha a che fare? Buongiorno. Un episodio, poi è stato determinante il contesto preciso, ora. Ora me lo ricorderò, però c'era un'ipotesi che in un dispaccio che era stato intercettato AF corrispondesse ad una certa posizione geografica, ad una certa città.
Un'isola come una torre.
E in pratica?
Stavano cercando.

Di convincere i generali che era imminente un attacco contro questo aloe però non avevano il libretto analisti informazioni a sufficienza.
Per poter affermare con certezza che AF corrispondesse, diciamo, a quell'approvazione al più utilizzato uno stratagemma.
Simularono l'assenza di atto si rivolge bene sull'atollo.
EE in pratica quello che è successo è che chi aveva.
Tedeschi che volevano attaccare la fede, ma praticamente mandavano uno spaccio cifrato in cui dicevano che questo posto era privo di acqua o stavano finendo le risorse di acqua e faccio.
Per appunto era privo di acqua, quindi in quel caso l'associazione fu immediata tra il posto.
Stato 5 e praticamente la.
Cifra prima AF.
E il problema?
Ancora una volta ragazzi, questo grazie è il che si era di fronte ad una cifratura di tipo deterministico.
Quindi allo stesso.
Ogni volta che avveniva una cifratura, questa cifratura aveva la forma a edile, però questa associazione permise appunto ai analisti di convincere i generali che effettivamente a Ezio rispondeva A quel compito, e quindi?
Felice di prepararsi all'attacco che stava per essere sferrato.
Paradossalmente dicendolo in maniera diversa, se io scrivo di cifratura fosse stato probabilistico, questa associazione non poteva essere inserita d'accordo.
Quindi ragazzi, sicuramente gli attacchi di tipo sono già in tempo, sono importanti, tra l'altro l'esempio questo ha a che fare veramente con la nostra frase quotidiana.
Ragazzi, immaginate che il vostro terminale per ragioni di sicurezza.
Cipri, tutto ciò che vuoi.
Tutto ciò che voi digitate quindi state utilizzando qualsiasi programma che manda dati da qualche parte e li cifra che è stata scelta se non avete scelto con un'altro terminale.
Allora sicuramente voi che potete fare potete scrivere, quindi scegliete.
Piedi, messaggi, Descrivi e potete vedere che.
Quindi potete raccogliere.
Messaggi.
Ci fra i messaggi ci fra, quindi potete costruire una lista?
Per poter sferrare eventualmente un attacco di tipo l'obiettivo, per esempio.
Quando al posto vostro scriva di qualche altro di capire quest'altra persona che cosa sta scrivendo, o di capire le informazioni parziali o semplicemente che gli obiettivi cercare una rottura totale del sistema.
Del.
Con l'obiettivo di recuperare, per esempio, la chiave che viene utilizzata ma.
Parlante 4 01:01:52
È un po' simile a quello che dovrebbero.
Fare da una settimana, se non sbaglio, e votare la Commissione europea, cioè contro, è una cosa.
Parlante 2 01:02:01
No, lei stava dando di un'altro tipo di problema.
Parlante 4 01:02:05
Cioè, prima ancora di inviare il no, no, no, no, allora quella è.
Parlante 2 01:02:09

Una questione un po' complicata, magari è una questione che.
È nata già intorno al 2001 Live l'aveva pensato di introdurre all'interno di tutti gli iPhone un meccanismo per poter individuare il.
La la presenza di eventuale di materiale breve pornografico.
Lui si riferisce, si rimettiamo. Ci sanno qualcosa del genere Child material of Music, qualcosa del genere. Mi ricordo la cipria.
E fondamentalmente funzionava in maniera funzionava in questo modo il sistema che la discorso non è tanto appunto su ogni cellulare viene scaricato una sorta di database con delle informazioni con degli hash. Vedremo cosa sono, non sono proprio gli hash che consideriamo noi.
Allora ci sono delle informazioni per cui quando un utente fa l'upload di un'immagine in drive o nel caso di Apple appunto.
Tra il virgole, cioè il plauso di virgolette, quello che accade è che viene effettuata una sorta di analisi sull'immagine.
Che un voucher viene spedito a qualche server nel momento in cui accade che un utente che ha materiale sempre pornografico.
Dico che fa l'upload di più roba di questo tipo.
Questi voucher?
Raggiungono il server quando il server ne ottiene una certa quantità. Quello che può andare a fare è andare ad aprire questi voucher e capire chi è l'utente, quindi di carpirne l'identità e dare alle autorità poi informazioni su questa persona.
Cioè il problema grosso è che appunto sul cellulare di ogni persona c'è un meccanismo che fa un'analisi delle foto che ci sono prima di effettuare l'upload e dà delle informazioni.
Questo sistema la Apple aveva l'aveva proposto questo ricordo bene intorno al 2000, 2000, 2020, 2021, però non hanno mai diffusione perché appunto ci sono stati un po' di primi, un po' di cose. Ora questo l'equivalente di questo sistema ho la possibilità di realizzare i sistemi del genere, è in discussione.
All'Unione europea. E sono stati diversi anche le uniformi con la comunità dei crittografi eccetera. Tra l'altro io avevo scaricato il documento grosso, documenti diciamo molto onerosi, ma ho avuto tanto il tempo diciamo di di di leggerli.
C'è stata un'opposizione abbastanza ferrea da parte della della della Comunità dippografica, perché pare che appunto questi sistemi diano poi la possibilità di poter violare quella che è la privacy livelli. Non c'è sempre un problema di trade off tra quella che è la privacy degli utenti, che è l'obiettivo, anche nobile, che invece quel tipo di sistema vuole cercare di raggiungere.
Diciamo rispetto alle cose di cui stiamo parlando al momento.
Ecco, a meno di non andare a pensare a un attacco di Edo, cioè sembra però non riservare i dettagli da questo tipo di.
Va bene, relativamente agli attacchi, è chiaro quello che vogliamo fare e perché sono una preoccupazione, perché questa era.
Questa è la l'informazione che voglio veicolare, cioè sono un pericolo concreto per uno schermo.
Domanda, come facciamo a modellarci la capacità di un avversario di disporre riciclati?
Corrispondenti ai messaggi di propria scelta.
Ragazzi, che ore sono?
10:15 vediamo fra 5 minuti di pausa.
Parlante 8 01:05:39
Allora ragazzi, però.

Parlante 2 01:05:42
Per evitare di fare.
Come l'altro giorno, poi 10 diventano 10, 15 io inizio non prima divinità.
7 minuti di 7 minuti.
Siamo tornati sul problema della modellazione.
Sì, è chiaro a tutti cosa intendiamo per attacchi, matricola, avversario, può scegliere un certo numero di messaggi, ottenere il citrato ad un certo punto però.
Il Comunicante Alice sceglie di sua sponda e autonomamente un messaggio è nocifero, lo invia e lo scopo dell'azzeramento.
Parlante 8 01:06:26
È quello di capire.
Parlante 2 01:06:29
Come facciamo a modellare la velocità dell'avversario, predisporre, decifrare corrispondenti ai messaggi di propria scelta.
Faccio una osservazione, diciamo di tipo generale, che.
In tutte le definizioni.
Fino ad ora avrà notato degli esperimenti?
Continueremo a fargli tutte le definizioni che daremo in grado di sostengono e in lui.
Un Challenge?
Sfida un avversario che cerca di avere successo.
In un determinato caso, questo è il modo in cui.
Abbiamo operato.
In molti casi fino ad ora e considerando poi l'esperimento, abbiamo espresso le garanzie di sicurezza, fondamentalmente in termini di fallimento dell'avversario all'interno dell'esperimento.
Spero quindi che siate convinti che gli esperimenti permettono di astrarre e modellare scenari reali.
In modo semplice.
Per modellare.
Un attacco di tipo soltanto. Ci dobbiamo allora introdurre, nell'esperimento, qualche cosa che permetta all'avversario di avere il cifrato in corrispondenza a messaggi che scelgono. E questa cosa che puoi riprodurre è un oggetto che chiameremo oracolo, quindi per noi un oracolo sarà una scatola nera che.
In questa applicazione specifica che stiamo considerando cifra messaggi usando una certa chiave K.
Ora le assunzioni che facciamo sono prima di tutto quell'avversario non conosce la chiave K nell'oracolo utilizza per cifrare?
L'avversario interagisce con l'oracolo inviando richieste di filtratura, che in generale chiameremo QUERY.
Specificato il messaggio e ottenendo in risposta la cifratura del messaggio M.
Se.
Lo schema di cifratura che stiamo considerando, che è implementato all'interno del miracolo, è randomizzato.
Duravo.
Per cui saranno lì sempre nuovi, quindi.
Sì.
Chiediamo l'orario della cifratura di uno stesso messaggio che vuole, otterremo cifrati diverse.

D'accordo.
L'avversario può inviare ad attivamente quante guerre.
Quante vuoi di Guess? Ovviamente se stiamo parlando di un algoritmo di tempo colinomiale significa che il numero di query che può inviare è quanto pure però è sempre coninomiale.
E adattivamente significa, come vedete, immaginare la cosa seguente, l'avversario può inviare un messaggio.
Ma poi arriva un messaggio ottieni cifrato.
Nella guerra successiva potrebbe anche tener conto della doppia messaggio cifrato che ha ottenuto e quindi costruire un messaggio in funzione di ciò che ha ottenuto.
E questa cosa la può fare anche nei bambini successivi, quindi può adattare le query di cifratura che fa l'oracolo tenendo conto della storia passata.
Benissimo, utilizzando il muracolo allora possiamo.
Posso aver qui il seguente esperimento?
Si.
La tripla che definisce uno schema di cifratura, si ha un avversario n al soglio. Il parametro di sicurezza.
Indichiamo calling a che ha come apice l'oracolo. Attenzione, questa è una notazione che sarà utilizzata in tutto il prosieguo. Che cosa un processo interattivo, quindi ha.
Elevato, diciamo all'orario, significa la cosa seguente che l'avversario ha ha accesso all'oracolo e le lo può interrogare quante volte vuole. Quindi ogni volta che sto scrivendo ha elevato alla o sto dicendo che ad un certo punto l'oracolo può vantare 101520 premio 100 query all'oracolo può andare delle risposte, continuare ad interagire con l'oracolo, dopodiché farà qualche cosa.
D'accordo.
In generale quindi questa annotazione significa che ha ha accesso all'oracolo e come garantirci qualche volta le esperienze che considereremo e chiamo? Guardate vendita KCPA per indicare questo? Modellando attacchi di micro CPA sarà il seguente.
Il Challenger, utilizzando l'algoritmo di generazione delle chiavi.
Scegli una chiave.
Mentre nella maggior parte dei casi geni dei casi, Gen è un algoritmo che sceglie le chiavi usualmente a caso dell'insieme delle possibilità, quindi sceglie questa chiave e il Challenger setta l'oracolo. Quindi che cosa significa predisponde l'oracolo affinché possa cifrare messaggi con l'algoritmo è utilizzato la chiave K che è stata scelta.
Quindi fondamentalmente l'oracolo viene settato con un'istanza dello schermo di ciclorità.
Va bene un secondo passo l'avversario.
Interagisce con l'oracolo, quindi questa.
Semplice relazione, indica il processo di interazione popolare.
Che durerà un certo po di tempo.
L'avversario manda un messaggio dorato, ottiene la risposta, manda un'altro messaggio, ottiene un'altra risposta, quindi raccoglie quelle che si sono le sue coppie quando si sente pronto.
Time out, un termine zero ed m uno che sono i due messaggi sui quali vuole essere sfidato da parte del Challenger.
E vale sempre la restrizione che devono avere la stessa tendenza.
Anche perché i riferimenti che abbiamo visto precedentemente, il Challenger sceglie a caso decifrare m zero moderne etico.
Cifra, il messaggio MDB con la stessa chiave con cui l'oracolo ha prodotto cifrature precedentemente.

Da.
All'avversario e guardate l'avversario.
Ancora una volta oh.
Decidere.
Tranquillamente.
Se il ciclo listone la cifra dura di 1E0DRQ, ma potrebbe anche applicare una qualsiasi altra strategia.
In base alla quale, prima di dare una risposta, interroga ancora l'oracolo, cioè, potrebbe avere necessità o potrebbe la strategia prevedere che l'avversario continua a raccogliere coppie? Messaggio cifrato?
D'accordo, in questo caso quindi l'avversario esegue per tutto il tempo che vuole.
E.
Ad un certo punto però si dovrà pronunciare e darà in auto con il bit il primo che è la sua.
Parlante 3 01:13:46
Scommessa su cosa incifrato di?
Parlante 2 01:13:48
Sfida, contiene se indovina al solito l'output dell'esperimento.
Sì, dice.
Fallisce l'autobus dell'esperimento, è zero.
Quindi.
Cosa ho modellato in questi esperimenti?
Ho modellato il fatto che l'avversario ha riesce ad avere coppie di messaggi citrati a volontà.
E l'ho fatto in una maniera diciamo abbastanza forte, perché l'avversario può interagire con l'orario sia prima di vedere il cifrato di suo interesse, quello che deve attaccare, sia subito dopo, nel senso che l'avversario, anche quando ha avuto il circuito, potrebbe cercare di costruire delle interrogazioni per l'oracolo di cifratura che dipendono in qualche modo dal cifrato che ha ricevuto.
In base AA qualsiasi strategia potete immaginare.
Quando è con te che è soddisfatto di questa generazione? Ad un certo punto però proverà ad indovina.
E come potete a questo punto del corso immaginare? Come faccio a definire uno schema di cifratura sicuro rispetto ad attacchi di questo genere?
Lo farò con la solita definizione, in cui però l'esperimento di riferimento è di questo e vi chiederò che ogni avversario efficiente.
Riesca a vincere dell'esperimento con probabilità.
Trascurabilmente migliore di un mezzo, quindi credo che la definizione non sorprenda nessuno. Uno schema di cifratura chiave privata a cifrature indistinguibili rispetto ad attacchi di tipo Chosen. Planitex che i ragazzi utilizzeremo sempre questo acronimo per gli attacchi, quindi diremo che uno schema il CTA sicuro se per ogni avversario efficiente esiste una funzione trascurabile tale che la probabilità dell'avversario abbia successo.
È appunto, un mezzo più qualcosa di trascurabile.
E al solito, ragazzi. Questa probabilità viene calcolata su tutti gli elementi di valorizzazione che sono presenti nell'esperimento, quindi in particolare, a è un algoritmo probabilistico, quindi può usare random B se USA 10 random B nella Stati Uniti suo codice per fare l'analisi dobbiamo tener conto dei random e all'interno dell'esperimento abbiamo visto che al solito.
Il Beach viene scelto a caso.
La chiave viene scelta attraverso la guerra, quindi ci sono.
Un po' di elementi casuali.

Di cui occorre tenere di vuoto.
Nell'analisi della probabilità.
OK.
È quello che voglio fare ora.
Insieme a voi.
Siete tutti convinti che questa nozione di sicurezza che sto dando ha ancora una volta come target l'invio di un'unica cifra?
Giusto.
Nel mio esperimento?
L'avversario ad un certo punto sceglie M0E31, quindi questa scelta lo dice con un vostro collega tempo fa.
È una scelta, è una strategia che noi usiamo nell'esperimento per cercare di mettere l'avversario nella migliore convinzione possibile.
Cioè stiamo supponendo che l'avversario sappia che quando Alice invia il messaggio a poco, quello che non controlla sa comunque a priori che il messaggio può essere uno di due.
E stiamo dicendo in questa condizione, anche sapendo che sta il messaggio è l'uno dei due.
Ricevendo il cifrato non riesce a capire se corrisponde all'uno o all'altro, però in questa definizione in tablet è la sicurezza di un unico messaggio, appunto di quello che è sottostante C.
Quindi, se volessi invece considerare.
Una nozione di sicurezza in cui lo schema può essere usato per l'invio di messaggi.
Come modificheresti l'esperimento, ragazzi?
Parlante 4 01:18:05
Sempre le liste.
Parlante 2 01:18:06
Come dice il posto colleghi sempre le liste.
Quello che potrei fare?
L'avversario potrebbe dare in autobus due liste, m grande zero M -0. Quindi i messaggi sono uguali accorti?
A sceglie di il challengersceglie.be decide se scegliere la prima lista o la seconda lista.
D'accordo e quindi sicuramente questa formalizzazione potrebbe essere estesa per dare una definizione di sicurezza rispetto ad attacchi di tipo CTA per messaggi con futuri.
In realtà.
Questa cosa funziona, quindi la risposta è corretta, però vi faccio vedere come si può fare in maniera più elegante.
Definendo.
L'esperimento.
Tramite l'uso di un oracolo diverso.
E la formalizzazione che sceglie il vostro libro e spero che vi convinca che stiamo modellando esattamente la stessa cosa, dando però all'avversario ancora più potere.
Vediamo se vi trovate.
Supponiamo di disporre di un oracolo che chiamo LR che sta per left. Orright quindi sinistra o destra e un attimo capiremo perché.
Che ha bisogno, diciamo, di due.
Informazioni che vengono.
Fissate prima dell'inizio dell'esperimento K, che è una chiave di cifratura EB che è un bit che stabilisce se.

I messaggi cifrati sono quelli di sinistra.
In una coppia o sono quelli di destra?
In particolare vediamo se di.
Se ti convince l'uso che facciamo di questo Ago al meglio esperienza quindi l'oracolo quando riceve in input due messaggi è da zero ed m uno.
Se il bit con cui è stato settato è zero, cifra n zero. Se il bit con il quale è stato settato è uno cifra n uno, però questa operazione viene fatta all'inizio, quindi poi lo danno o cifre sempre m zero o.
Parlante 6 01:20:24
Cifre sempre in questo modo, l'avversario.
Al quale due dei due.
Parlante 2 01:20:29
Messaggi sta cifrando l'avversario, non sa quale bit è stato scelto, sarà proprio questo il compito dell'avversario. Vediamo se ci troviamo.
Non posso definire questo esperimento, c'è sempre il changer che il file setup dell'esperimento utilizzando l'algoritmo di generazione della chiave.
Genera una chiave.
Scegli un beat a caso.
Setta l'oracolo, quindi questa è l'operazione che fa il Challenger e permette all'avversario di interagire con l'orario.
In base a questa mutazione, abbiamo detto che dal messaggio di interagire con l'orario tutte le volte che.
Questa volta, per interagire con l'oracolo, gli deve mandare una pubblica di messaggi.
M zero ed M uno.
E riceverà dall'oracolo.
Il cifrato di uno dei due.
Ovviamente, però.
Sia le cave di cifratura che il TIC, come abbiamo detto.
L'avversario interagisce con l'oracolo tutte le volte che vuole.
E ad un certo punto va in output.
Il biglietto?
Il bit di primo.
E appunto il suo tentativo di capire questo orario che cosa sta citando, se l'elemento di sinistra, le o l'elemento diverso?
Se l'avversario indovina l'altro dell'esperimento tecnico?
Segno fallisce, l'outlet dell'esperimento è zero. E quello che vi voglio comunque.
Quello che vuole dettare di fare ora è convincervi.
Tutti quanti.
Così compatto con questo oracolo.
Coglie perfettamente l'esperimento.
Di sicurezza, c'è un server firedex rispetto all'invio di messaggi utili.
Per quale motivo?
Ragioniamoci e raggiunse nell'attacco se vediamo un esperimento precedente.
Che l'esperimento precedente l'avversario può raccogliere in qualsiasi momento, sia prima che dopo cifrati di messaggi di sua scelta.
D'accordo.
In questo esperimento, come fa l'avversario a cogliere messaggi?
Cifrati di messaggi di sua scelta.

Voi ci pensate un attimo, è molto semplice, basta che quando invia i due messaggi 1 0 R uno.
Invio uguale quindi.
Se sceglie coppie del tipo MM.
E fa questa interrogazione all'oracolo che cosa qui ottiene la cifratura del messaggio è.
D'accordo quindi sicuramente dell'argento con l'oracolo con coppie.
I messaggi uguali non riesce a raccogliere.
Coppie, messaggi, ciprali, quindi riesce ad ottenere tutte le informazioni che otterrebbe nell'attacco.
Condividendo ciò sembrato perfetto.
Nella estensione del messaggio multipli, che cosa diceva il vostro collega? Questo basta che togliamo m zero di m uno e ci mettiamo una lista M 0 ° ed una lista M 1 °. Dopodiché il Challenge sceglie se ci fate la lista di destra o la lista di vista.
Grazie.
Una volta che l'avversario qua ha terminato di raccogliere coppie, messaggio cellulare può cominciare ad inviare coppie di messaggi diversi M0M8M0M1.
Puoi inviare quanti messaggi, quante copie vuole e in questa seconda fase l'interazione con l'oracolo rappresenta esattamente.
L'invio in qualche modo al challenger delle due liste di messaggi?
Che verranno o.
E il bit zero?
Verrà decifrato il messaggio?
Della privatista, se emette uno verrà pubblicizzato i messaggi della seconda lista.
Vi trovate?
Qual è il svantaggio di questa formalizzazione rispetto a quello precedente?
In quello precedente, l'avversario.
Sceglierebbe M zero ed M uno, le due liste tutte.
Quindi sarebbe.
Trattato, se ci pensate un attimo, di tipo statico, perché io scelgo l'egoista.
E le do all'avversario.
In questo esperimento, invece?
Guardate che ho introdotto un elemento di dinamicità. Perché? Perché l'avversario qui può scegliere le prime due enti della lista, diciamo quindi m zero del M uno. Questi sono i primi messaggi delle liste, dopodiché.
A seconda di il ciclato che ha ricevuto può scegliere il nuovo, i ben zero del nuovo M uno, quindi le due liste.
È che lui sta costruendo, in questo caso sono liste in cui lui può cercare di introdurre anche delle dipendenze in base a qualche strategia o di città.
Parlante 9 01:25:41
Successivamente, nel successivo OA destra OA sinistra come.
Parlante 2 01:25:45
Può scegliere a seconda del ciclato che ha ricevuto, quindi il nuovo m zero e il nuovo m uno, introducendo qualche differenza.
Cosa che invece nella prima formatizzazione a cui abbiamo pensato.
Non è.
Fattibile. Perché? Perché io scelgo tutto l'importo.
Quindi vi vorrei convincere del fatto che questa formalizzazione prima di tutto.
Voglio esattamente.

Il contesto di un attacco Cosetta.
Compie i messaggi uguali riesco ad ottenere cifrati messaggi iniacie quindi stommo dell'anno in attacco di tipo josephine, e sto anche cercando di convincervi e utilizzando invece l'oracolo nella forma naturale, cioè con due messaggi diversi. In questo esperimento è come se io ad un certo punto sfidassi il Challenger con due liste di messaggi.
Solo che.
Il primo caso, quello che abbiamo visto, le due liste vengono scelte tout e il Real challenger, qui invece la costruzione della lista avviene danno maggiore potere all'avversario, il quale può decidere le nuove enti delle liste.
Rendo conto anche dei riciclati che ha appena diciamo creator.
E spero che vi sia anche chiaro che alla fine se indovina il Libro il VIP, ovvero se indovina.
Durante l'o LR che cosa cifra se l'elemento diverso, l'elemento di sinistra?
Implicitamente cosa stiamo dicendo? Che sta rompendo lo schema di cifratura, cioè sta accadendo se esso sta decifrando i messaggi di destra o di sinistra, quelli della prima o della seconda lista, cioè fondamentalmente.
Riciclaggio per il consumo di sicurezza.
Giusto.
Ti ho convinto ragazzi?
Perché ragazzi, se vi ho contribuito in questa slide ho riportato.
Esattamente quello che dicevo.
Differenze con l'approccio precedente l'avversario che le le cifrature di n inviandole coppie, le coppie meno 0IR1I sono scelte ad attivamente invece che insomma.
Quindi questo esperimento mi permette di modellare.
A parte che questo esemplare ed in particolare ci mi permette di modellare un contesto in cui richiedo la sicurezza rispetto all'invio di messaggi pubblici.
Quindi mi permette di se riesco a provare con uno schema raggiunge questa definizione lo posso usare tranquillamente per l'invio di messaggio volevo?
Che credo, spero di sorprenda positivamente.
La definizione è quella che ci aspettiamo tutti quanti.
Cioè uno schema di psicologia a ciprodurre esempi e indistinguibili rispetto ad attacchi di tipo.
Semplice, se ogni avversario che tenta.
Di vincere nell'esperimento ha probabilità trascurabilmente milioni e mezzo.
E si può dimostrare che.
Se lo schema è CPA sicuro per cifrature multiple.
Ovviamente.
ECPA sicuro per l'invio di un unico messaggio. Perché? Perché ancora una volta.
Siamo considerando il caso in cui.
Nelle liste come se ci fosse un nuovo messaggio, ma la cosa che ci interessa è che in questo caso vale anche l'inverso. Quindi mentre per la nozione di indistinguibilità vi ho mostrato un controesempio stamattina glielo faceva vedere che indistinguibilità rispetto a un messaggio singolo non implica indistinguibilità rispetto al messaggio multipli. In questo caso invece se uno schema è c la sicure per messaggio singolo.
ECPA, seguito anche dai messaggi utili.
Il che significa che questo è un grosso vantaggio che, dato un'offerta, basta che lo coloriamo CTA sicuro per essere.
Tranquilli, per essere convinti che lo possiamo usare per messaggi utili.
Quindi questo è il risultato importante.

L'altra implicazione?
Che ci serve anche dal punto di vista costruttivo, anche se poi avremo tecniche più efficienti per costruire schemi di ciclatura CTA. Silvia è la seguente.
Se.
Uno schema.
E ci ti assicuro per messaggi di lunghezza fissata, per esempio.
Anche per messaggio di un mip posso utilizzare questo schema per costruire un'altro permessaggi di lunghezza maggiore, quindi nel caso proprio estremo?
Se riesco a costruire uno schema?
CTA sicuro per messaggi più B deposto, poi costruire uno per messaggi di lunghezza, di Rai, di lunghezza etica e la tecnica costruttiva è praticamente questa.
L'algoritmo di generazione delle chiavi resta lo stesso.
La cifratura del messaggio di lunghezza arbitraria diventa la giusta posizione delle cifrature per i bit del messaggio e la decifratura, come potete immaginare, diventa la decifratura dei singoli bit del messaggio.
Come ve lo immaginate? Questa non è una tecnica molto efficiente perché il cifrato di n in questo caso diventa un ciclato molto grande, quindi abbiamo altre tecniche. Però da un punto di vista teorico questa cosa funziona. Perché funziona. Pensate il fatto, perché se vale la proprietà di quello che stavo parlando un attimo fa, e cioè che moschea ci sia sicuro per messaggio singolo è sicuro per messaggi pubblici.
Ragazzi.
In questo schema questi sono messaggi utili.
Cioè è vero che io li sto vedendo come la cifratura di un unico messaggio, però sono cifrature.
Quindi big bit diverso quindi se lo schema è sicuro anche per messaggi luci complessivamente.
Questa.
Cifratura è la posso vedere come la cifratura sicura CPA sicura per un messaggio di ricorso arbitraria.
D'accordo.
Benissimo questa prova, ragazzi della equivalenza. In realtà sul vostro testo verrà riportata quando concederemo schede di cifratura a chiave pubblica.
E la prova è fondamentalmente la stessa, però il nostro testo, nel contesto simmetrico, non nell'altro, agisce.
Accredito diver fede al momento che effettivamente queste due non sono.
Sono equivalenti.
EEA questo punto.
Probabilmente se siete stati mi fermerei completerei domani mattina, vedete perché a questo punto le nozioni che abbiamo date, quindi abbiamo considerato.
Abbiamo considerato che il piattaforme di CPAE.
Quello che voglio cercare di.
Guardi, io vedo domani mattina, è come possiamo costruire, che decifrazione.
E in particolare avremo bisogno di un po' strumento che è rappresentato appunto dalle funzioni pseudo casuali, dalle permutazioni di pseudo casuali. Quindi domani mattina la prima volta di definire questi incertezza e se il tempo sarà sufficiente vi fornirò anche un esempio di sistema.
D'accordo.