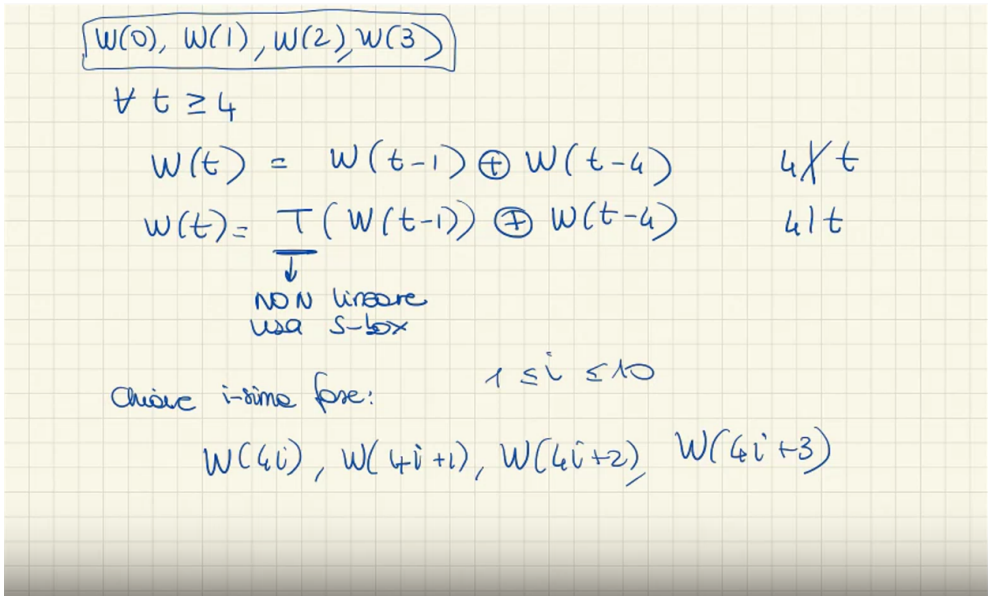
Q&A Crittografia

- Descrizione del funzionamento dell AES
  - Pagine 116 e 117 del libro
- Calcolo che sta dietro alla creazione della tabella della SBOX dell'AES
  - La S-Box applicata ad un byte X restituisce X^-1, ovvero l'inverso moltiplicativo di X in GF(2^8) (Campi finiti di Galois), dove l'addizione è eseguita modulo 2 (xor) e la moltiplicazione invece modulo 8. (https://it.wikipedia.org/wiki/S-box_del_Rijndael)
- In quale altra operazione interviene la SBOX dell'AES (nella costruzione della sottochiave)
  - Nella costruzione della sottochiave. Si prende ad esempio una chiave k di 128 bit, si organizza logicamente in una matrice K di 4 x 4 byte per colonne (come il messaggio) ed ogni cella è esattamente un byte. In ogni fase la matrice K viene "aggiornata" tramite l'S-Box, generando una nuova sottochiave locale a quella fase. Dato W(i) la colonna i della matrice K (0 <= i <= 3):
  - 

- In quali ipotesi il one time pad è perfetto, indica la dimostrazione formale
- Se mai ci sarà l'avvento del computer quantistico, che effetto avrebbe sui cifrari perfetti e in particolare sul onetimepad (nessuna) e sull'AES e in generale sui cifrari simmetrici?
- Come cambiare un AES a 256 bit in presenza di computer quantistici? (curiosità, domanda senza peso)
  - Aumentare la lunghezza delle chiavi a 512 bit
- Algoritmo risoluzione logaritmo discreto e sua complessità
- Perchè le curve ellittiche stanno soppiantando la cifratura asimmetrica
- Con l'avvento della macchina quantistica, che ne sarà dello lo scambio di chiavi con le curve ellittiche?
- Il problema del logaritmo discreto su macchina quantistica diventa facile, grazie all'algoritmo di Shor con alcuni accorgimenti
- Dimostrazione di correttezza di RSA nel caso in cui il messaggio e il modulo non sono coprimi
- Cosa sono i generatori crittograficamente sicuri e presentare un esempio
  - Un generatore si dice crittograficamente sicuro se passa il test di prossimo bit, ovvero se un crittoanalista, osservando la sequenza di bit, non può prevedere con probabilità significativamente maggiore di ½ quale sarà l'i+1-esimo bit, conoscendo l'i-esimo bit e tutti i precedenti. Un esempio di generatore crittograficamente sicuro è il BBS, in quanto calcola un predicato *b* su ogni *f(x)*, dove ogni f(x) dipende, in un certo senso, dalla precedente. Inoltre, la sequenza casuale calcolata viene restituita in output in ordine inverso.
- Influenza della quantistica sulla cifratura simmetrica
- Koblitz, Vigenere
- Confusione e diffusione, quali dei due principi implementa la sbox (soprattutto la confusione)
- Complessità secondo Kolmogorov
- Esistono e quante sono le sequenze casuali?

- Posso stabilire se una sequenza è casuale?
- Teorema Shannon nei cifrari perfetti (N° chiavi >= N° messaggi)
- Protocolli zero-knowledge, Fiat Shamir: perchè bit e è importante
- Attacchi meet-in-the-middle
- Protocollo BB84
- Crittoanalisi statistica
- Attacchi a RSA (quando p-q è piccolo, se più utenti hanno lo stesso valore di e, se più utenti hanno lo stesso n)
- Protocollo Dh per scambio di chiavi (sia in algebra modulare che curve ellittiche)
- Scambio di messaggi cifrati su curve ellittiche
- Serve una macchina quantistica per il BB84?
- RSA cifrari ibridi
- Crittoanalisi statistica
- Vigenere, come si fa diventare più robusto? si può trasformare in un cifrario perfetto, come?
- Chiave pubblica su curve ellittiche
- Algoritmo di Koblitz, costo?
- Protocollo su curve ellittiche
- Correttezza RSA
- Attacco RSA con n scelto uguale
- Come confrontare la sicurezza dei cifrari al livello computazionale
- Come si può ricavare il valore k quando si usano algoritmi sulle curve ellittiche basandosi sui punti P e Q?
    - Per poter trovare k è necessario risolvere il problema del logaritmo discreto su curve ellittiche, che richiede tempo esponenziale in quanto è necessario provare tutti i valori di k > 1 fino a trovare quello per cui Q = k P.
- Conosciamo già il protocollo DH per la costruzione (e lo scambio) di una chiave di sessione. Supponiamo uno scenario in cui tre utenti Alice, Bob e Charlie vogliano creare una chiave di sessione per una comunicazione tri-direzionale. Come va modificato il protocollo DH per far ciò che questo avvenga?
    - Esattamente come nel normale protocollo DH, i tre interessati scelgono p primo molto grande e g generatore per Zp*, che sicuramente esiste per un teorema. Poi, ciascuno di loro genera la coppia valore pubblico e privato come segue:
    - Alice: A = g^x mod p
    - Bob: B = g^y mod p
    - Charlie: C = g^z mod p
    - Dove x, y e z sono tutti minori di p e scelti a caso dai tre. Per costruire la chiave di sessione bisognerà procedere nel seguente modo:
    - Alice manda A a Bob. Bob calcola A^y = U. Bob manda U a Charlie, che si calcola U^z = g^(xyz). Così Charlie ha costruito la chiave di sessione. Il ragionamento è analogo per Alice e Bob.
- Sequenze casuali, in particolare che cos'è la Complessità di Kolmogorov, come ci si libera dalla scelta di un particolare sistema di calcolo S_i e perché le sequenze casuali lunghe n, fissato un valore n per la lunghezza delle sequenze binarie, sono molte di più di quelle non casuali.
- AES, descrizione generale; qual è l'importanza delle fasi 2 e 3, cosa realizzano (diffusione?)
- Protocollo BB84: con e senza crittoanalista nel mezzo alla comunicazione. QBER
- Cifratura perfetta: definizione, ipotesi necessarie per dimostrazione, dimostrazione, cosa succede se cade ipotesi in cui si chiede che tutti i messaggi siano possibili?
- RSA: come può essere attaccato RSA se p e q sono simili?
- BB84, perché si usano due basi di polarizzazione?
- Come un crittoanalista può attaccare il protocollo
- Come un crittoanalista può attaccare il protocollo senza "lasciare traccia" e cosa possono fare gli interlocutori per prevenire questo accatto
- In quali classi si dividono i cifrari storici
- Cosa ci dice l'analisi statistica in riferimento ai cifrari storici, come ci aiuta ad attaccarli
- Quali altri cifrari storici conosciamo? (trasposizione)
- Come si attacca un cifrario a trasposizione

- Quali sono i problemi dei cifrari a chiave pubblica
- Come si configura un attacco man in the middle nel caso di un cifrario a chiave pubblica
- Che ruolo svolgono le funzioni one-way nell'ambito dei generatori crittograficamente sicuri, fare un esempio
- Test di prossimo bit
- Come un generatore crittograficamente sicuro impedisce ad un crittoanalista di prevedere l'i+1-esimo bit
- Correttezza RSA con n e m NON coprimi
- Protocollo BB84:
    - cosa cambia se Eve riesce a prevedere le basi che sceglierà Alice (Eve per non essere scoperta userà le basi di Alice)
    - Cosa cambia se Eve riesce a prevedere le basi che sceglierà Bob (Eve per non essere scoperta sceglierà le basi di Bob)
    - Come fanno a generare bit casuali? (Devono usare un generatore di bit casuali che supera il test di prossimo bit ad esempio il generatore BBS)
- Dimostrazione th. Shannon
- Dimostrazione che One Time Pad è perfetto
- Attacco RSA con n uguale
- Quando una sequenza è casuale secondo Kolmogorov
- Esistenza di sequenze casuali con dimostrazione
- Fiat-Shamir e quali sono i vantaggi rispetto al protocollo di identificazione visto in precedenza
    - r viene generato dall'utente e non dal sistema, questo non permette al sistema di scegliere appositamente r per avere informazioni sulla chiave privata)
- Protocollo di autenticazione (cos'è il MAC)
- Generatore di numeri pseudo-casuali crittograficamente sicuri
- Dimostrazione teorema di Shannon
- Cifrari ibridi, perché permettono di eliminare le debolezze dei cifrari asimmetrici
    - i cifrari asimmetrici sono molto meno efficienti rispetto a quelli simmetrici e sono esposti agli attacchi chosen plain-text, perciò utilizzandoli solo per lo scambio di chiavi si riduce l'inefficienza(perché si usano "poco") e visto che le chiavi scambiate sono sequenze generate (pseudo)casualmente, queste non possono essere attaccate tramite chosen plain text)
- Dimostrazione correttezza RSA, a scelta uno dei due casi
- Protocolli di firma digitale, perchè nel protocollo 2 avrebbe poco senso cifrare direttamente il messaggio anziché la firma?
- Generazione numeri primi, come può essere fatta? (MIller-Rabin) Se fallisco il test è difficile trovarne uno? (vuole essere detta il discorso della distribuzione dei primi in un intorno logaritmico di N)
- Caratteristiche delle funzioni hash one-way
- Mostrare l'attacco al RSA tramite utenti con uguale valore di e.