Programma di Crittografia A.A. 2018/2019

1. Funzione φ di Eulero. Generatori dei gruppi ciclici finiti. Formula $\sum_{d|n} \varphi(d) = n$. Unità di un anello. La funzione di Eulero è moltiplicativa.
2. Il gruppo moltiplicativo di un campo finito è ciclico.
3. Radici primitive dell'unità. Richiami sui campi finiti. Morfismo di Frobenius.
4. Residui quadratici. Quadrati in un campo finito.
5. Simbolo di Legendre e sue proprietà.
6. Simbolo di Legendre per il primo 2.
7. Teorema di reciprocità quadratica.
8. Simbolo di Jacobi. Simbolo di Jacobi per il 2. Teorema di reciprocità per il simbolo di Jacobi.
9. Operazioni elementari. Algoritmi polinomiali.
10. Stima del numero di *bit operations* per somma e prodotto. Cenni all'algoritmo di Karatsuba.
11. Complessità del calcolo delle potenze modulari.
12. Complessità dell'algoritmo di Euclide esteso.
13. Equivalenza computazionale.
14. Equivalenza computazionale tra fattorizzazione e calcolo di $\varphi(pq)$.
15. Estrazione di radici quadrate in campi finiti.
16. Sistemi crittografici classici. Sostituzione monoalfabetica.
17. Sistema di Vigenere e sua analisi.
18. Cifrature a flusso. Sequenze ricorsive.

19. Il tratto iniziale di una sequenza ricorsiva su un campo finito si ripete.

20. Costruzione di sequenze ricorsive di periodo massimo.

21. Cifrature a blocchi. Modo ECB e CBC.

22. Logaritmo discreto. Protocollo di Diffie-Hellman.Protocollo di Massey-Omura. Protocollo di ElGamal.

23. Algoritmo di Shanks per il calcolo del logaritmo discreto.

24. Algoritmo di Hellman-Pohlig-Silver.

25. Descrizione di RSA.

26. Crittosistema di Rabin. Forzare Rabin equivale a fattorizzare il modulo.

27. Testa o croce a distanza. Firma Cieca. Protocollo ANDOS.

28. Fattorizzazione del modulo n di un RSA, noto un intero m tale che $x^m = 1$ per ogni $x \in U(\mathbb{Z}/n\mathbb{Z})$.

29. Frazioni continue finite. Ogni razionale si rappresenta come una frazione continua finita. Teorema di Wiener (attacco ad RSA basato su un esponente privato basso).

30. Schema di firma di Lamport. Schema di Bos-Chaum.

31. Schema di van Heyst-Pedersen.

32. Schema di Chaum -van Antwerpen.

33. Funzioni hash e di compressione. Funzioni hash debolmente e fortemente senza collisioni. Funzioni hash one-way.

34. Una funzione Fortemente Senza Collisioni è One Way.

35. Funzione di compressione di Chaum-van Heyst-Pfitzmann.

36. Funzioni hash da funzioni di compressione.

37. Paradosso dei compleanni.

38. Divisione di segreti. Schemi a soglia. Protocollo di Shamir per la divisione di segreti. Polinomio di Lagrange.

39. Protocolli a conoscenza zero. Prova della conoscenza di radici quadrate modulo $n = pq$.

40. Schema di identificazione di Feige-Fiat-Shamir.

41. Prova della conoscenza di un logaritmo discreto.

42. Test di primalità. Numeri di Carmichael. I numeri di Carmichael sono liberi da quadrati. Un numero libero da quadrati è di Carmichael se e solo se $p - 1 \mid n - 1$ per ogni primo p che divide n. I numeri di Carmichael hanno almeno tre divisori primi.

43. Pseudoprimi di Eulero. Esiste sempre una base rispetto alla quale un numero composto non è pseudoprimo di Eulero.

44. Test di Solovay-Strassen.

45. Fattorizzazione di Fermat.

46. Metodo ρ di Pollard.

47. Metodo $p - 1$ di Pollard.

48. Curve ellittiche. Gruppo di una curva ellittica.

49. Codifica di messaggi come punti su curve ellittiche.

50. Cenni al metodo di fattorizzazione di Lenstra.