NIST College Banepa

Department of BScCSIT

5th Semester

Cyrptography

Tutorial 3: Review Questions

Review Questions:

1. Define an algebraic structure and list three algebraic structures discussed in this chapter.
2. Define a group and distinguish between a group and a commutative group.
3. Define a ring and distinguish between a ring and a commutative ring.
4. Define a field and distinguish between an infinite field and a finite field.
5. What does a field have, that an integral domain does not? Why is $\mathbf{Z}_n$ not an integral domain?
6. Show the number of elements in Galois fields in terms of a prime number.
7. Give one example of a group using a set of residues.
8. Give one example of a ring using a set of residues.
9. Give one example of a field using a set of residues.
10. List the three class of polynomial arithmetic.
11. Show how a polynomial can represent an n-bit word.
12. Define an irreducible polynomial.
13. Find Multiplicative inverse of each nonzero element in Z6.
14. Distinguish between a modern and a traditional symmetric-key cipher.
15. Explain why modern block ciphers are designed as substitution ciphers instead of transposition ciphers.
16. Explain why both substitution and transposition ciphers can be thought of as permutations.
17. List some components of a modern block cipher.
18. Define a P-box and list its three variations. Which variation is invertible?
19. Define an S-box and mention the necessary condition for an S-box to be invertible.
20. Define a product cipher and list the two classes of product ciphers.
21. Distinguish between diffusion and confusion.
22. Distinguish between a Feistel and a non-Feistel block cipher.
23. Briefly define a nonsingular transformation.
24. Why is it not practical to use an arbitrary reversible substitution cipher?
25. Which parameters and design choices determine the actual algorithm of a Feistel cipher?

26. What are the critical aspects of Feistel cipher design?
27. Distinguish between differential and linear cryptanalysis. Which one is a chosen plaintext attack? Which one is a known-plaintext attack?
28. Distinguish between a synchronous and a nonsynchronous stream cipher.
29. Define a feedback shift register and list the two variations used in stream ciphers.
30. How many rounds are used in AES and what does the number of rounds depend on?
31. What are the four steps that are executed in a single round of AES processing?
32. What is the purpose of S-Box in DES?
33. Even though we have a strong algorithm like 3-DES, still AES is preferred as a reasonable candidate for long term use. Why?
34. What is the difference between Rijndael and AES?
35. What is the purpose of the **State** array?
36. How is S-box constructed?
37. Des encryption was broken in 1999. Does that make this an unimportant cipher? Why do you think that happened?
38. What is triple encryption?
39. What is a meet-in-the-middle attack?
40. How may keys be used in triple encryption?
41. State the principle of Block cipher operation and list its different variation.

©Date of Submission: 25th Sep, 2023