NIST College Banepa

Department of BScCSIT

5th Semester

Cyrptography

Tutorial 4: Practice Questions

Practice Questions:

1. What is Euclid's algorithm for finding the GCD of two numbers? Explain.
2. Extended Euclidean Algorithm. Use this algorithm to test whether any two number n1, n2 are co-prime or not?
3. Calculate the result of the following if the polynomial are over GF(2):
   i. $(x^4 + x^2 + x + 1) + (x^3+1)$
   ii. $(x^4 + x^2 + x + 1) – (x^3+1)$
   iii. $(x^4 + x^2 + x + 1)$ x (x^3+1)
   iv. $(x^4 + x^2 + x + 1) / (x^3+1)$
4. The notation Z_n stands for the set of residues. What does that mean? Why is Z_n not a finite filed? Explain.
5. Find the result of the following operations:
   i. 27 mod 5
   ii. 36 mod 12
   iii. -18 mod 14
   iv. -7 mod 10
   v. -13 mod 7
6. What is $(02)^{-1}$ in $GF(2^8)$.
7. the multiplicative inverse of 11 in Z_{26} using extended Euclidean algorithm?
8. In $GF(\mathbf{2^4})$, find the inverse of $(\mathbf{x^2 + 1})$ modulo $(\mathbf{x^4 + x + 1})$. *Ans*: $x^3 + x + 1$
9. In $GF(\mathbf{2^8})$, find the inverse of $(\mathbf{x^5})$ modulo $(\mathbf{x^8 + x^4 + x^3} + 1)$. *Ans*: $x^5 + x^4 + x^3 + x$
10. Prove that $(\mathbf{x})$ and $(\mathbf{x} + 1)$ are irreducible polynomials of degree 1.
11. Prove that $(\mathbf{x}^2 + \mathbf{x} + 1)$ is an irreducible polynomials of degree 2.
12. Prove that $(\mathbf{x}^3 + \mathbf{x}^2 + 1)$ is an irreducible polynomials of degree 3.
13. What do you mean by a "Feistel Structure for Block Ciphers"? Explain.
14. What is the purpose of S-Boxes in DES? Prove that DES satisfies complementation property?

15. How IDEA operates on 64-bit blocks using 128-bit key? Describe each round of operations that IDEA follows to generate ciphertext of a 64-bit input message block.
16. Let's go back to the first step of processing in each round of AES. How does one look up the 16x16 S-box table for the byte-by-byte substitution?
17. Briefly describe about MixColumns and AddRoundKey stages in AES. How many bytes in a state are affected by ShiftRows round?
18. Compute the output of the MixColumns transformation for the following sequence of input bytes "A1 B2 C3 D4." Apply the InvMixColumns transformation to the btained result to verify your calculations. Change the first byte of the input from "A1" to "A3" perform the MixColumns transformation again for the new input, and determine how many bits have changed in the output.
19. Compare AES and DES.

©**Date of Submission**: 3rd Oct, 2023