Information and Network Security

Sheet 1 — CSE, SGSITS Indore

Assignment2: Mathematics of Symmetric-Key and Asymetric-Key cryptography, Modern Symmmetric-Key Ciphers, DES, AES, Assymetric-Key Cryptography

NOTE: Write answer in copy with name, enroll. number, sign., handwritten page number in sequence in each page. Scan all pages in sequence and upload only one .pdf file. You can use Virtual Cryptography Lab of IITH if given problems are relevant.

1. (a) Which of the following is (are) a valid Galois field and why?
   - (i) GF(12)
   - (ii) GF(13)
   - (iii) GF(16)
   - (iv) GF(17)
   - (v) GF(19)

   (b) For each of the following n-bit words, find the polynomial that represent that word:
   - (i) 10
   - (ii) 100001
   - (iii) 10010
   - (iv) 00011
   - (v) 1001101

2. (a) Find the result of the following operations:
   - (i) $(01001101) \oplus (01001101)$
   - (ii) $(01001101) \oplus (10110010)$
   - (iii) $(01001101) \oplus (00000000)$
   - (iv) $(01001101) \oplus (11111111)$

   (b) A message has **n** characters, where n refers the last 5 digit number of SGSITS student's enrollment number. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks.
   Note: If enrollment number is "0801CS171031", n = 71031; if enrollment number is "0801CS183d02", n = 18302.

   (c) (i) Decode the word 010 using a 3 x 8 decoder.
   - (ii) Encode the word 00100000 using 8 x 3 encoder.

3. (a) Answer the following questions about S-boxes in DES:

    (i) Show the result of passing 110111 through S-box 3.

    (ii) Show the result of passing 001100 through S-box 4.

    (iii) Show the result of passing 000000 through S-box 7.

    (iv) Show the result of passing 111111 through S-box 2.

   (b) Draw the table to show the result of passing 000000 through all 8 S-boxes in DES. Do you see a pattern in the outputs?

   (c) If the key with parity bit (64 bit) is **0123 ABCD 2562 1456**, find the first round key in DES.

4. (a) List the criteia defined by NIST for AES.

   (b) What do you mean by lightweight cryptography? Why is it required in current 21^{st} century world?

5. (a) Find the largest prime factor of the following composite integers: 100, 1000, 10,000, 100,000, and 1,000,000. Also find the largest prime factor of 101, 1001, 10,001, 100,001, and 1,000,001.

   (b) Find the value of $\phi(29)$, $\phi(32)$, $\phi(80)$, $\phi(100)$, $\phi(101)$.

   (c) Suppose Alice and Bob want to establish a shared secret key by executing the Diffie-Hellman key exchange protocol. First, they agree to use a modulus p = 13 and a generator g = 7. Alice then chooses a as her secret integer and sends Bob $A = g^a$ mod p = 8. Suppose Bob chooses 3 as his secret integer and sends Alice B = g^3 = 5 mod p. What is a shared secret between Alice and Bob?

   (d) In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is (e= 5, n=35). What is the plaintext M?

   (e) Write short notes on MD5, SHA-1, HMAC, and PKI.

6. Get the User's Login Email and Password by performing the Phishing attack using the fake Facebook site.(Hint: Use the SEtool Kit available in Kali Linux)

7. (a) Configure any XSS vulnerable website like DVWA or WebGoat in your local machine and write the script to perform the following XSS attack:

    (i) Reflected XSS

    (ii) Stored XSS

    (iii) Session Hijacking

   (b) Configure any SQL injection vulnerable website like DVWA or WebGoat in your local machine and perform the following operations:

    (i) Login in the target website

    (ii) CRUD Operation

8. Create a VPN using the IP Security protocol and also analyse it using the packet tracer.

9. How to configure a firewall for a small company? List out the steps with explanation? Write a short note on HPING/Firewalk – a firewall analysing tool.

10. Write a short note on SNORT – an IDPS. What are its features? Explain the process to install the SNORT.

11. What is ORACLE DBSAT? What does DBSAT check? How to install DBSAT, explain with steps?