Homework 3

Please put your solutions in a .doc, .docx or .pdf to CSNS by 11:59pm, Monday 03/16.

Total points: 10

---

1. (2pt) S-AES (Show all the results in hexadecimal)
   a) Generate the three round keys based on the key 1001 1111 0100 0010
   b) Encrypt the data block 0101 0110 1101 0011
   c) Decrypt the ciphertext block 0010 1111 0001 1001

2(1pt). Find the results of following, using Fermat's little theorem or Euler's theorem.

a) $15^{116060} \bmod 53$

b) $49^{-1} \bmod 416$

c) $101^{-1} \bmod 598$

d) $97^{-1} \bmod 1056$

e) $45^{1441251} \bmod 546$

3(1.5pt). RSA.

1) How to generate a key pair for Alice and Bob respectively? Both primes they pick should be greater than 100 and smaller than ~~1000~~ 300. Click here for a list of primes. Two or more students who select the same primes are considered cheating.

2) Suppose Alice sends plaintext P=113, how does she encrypt and what's the ciphertext C? After Bob receives C, how does he decrypts it to get the plaintext P?

3) Suppose Bob sends plaintext P=113, how does he encrypt and what's the ciphertext C? After Alice receives C, how does she decrypts it to get the plaintext P?

4) Suppose Alice sends plaintext P=113, how does she sign it and what are sent to Bob. How does Bob verify the signature?

5) Suppose Bob sends plaintext P=113, how does he sign it and what are sent to Alice. How does Alice verify the signature?

4(1pt). In ElGammal, given the prime p = 1327, e1= 5, choose d=512 r=103.
a) Calculate e2 and encrypt the message "phone"; use 00 to 25 for encoding.
b) Suppose the receiver receives the following ciphertext pairs(c1,c2): (1298,421) (1298, 874) (1298, 1231) (1298, 341), describe how to decrypt them to find the original plaintext? (note: a and b are independent questions.)

5(1.5pt). Use the Rabin cryptosystem with p = 43 and q = 31
a) Encrypt P = 28 to find the ciphertext
b) Use the Chinese Remainder Theorem to find four possible plaintexts

---

6(1pt). ElGamal signature scheme. Let p=881, e1 = 3, d=61. The random value r is 7.
a) Find e2 and the signature of the message M=300.
c) Verify the signature (show all the intermediate results).

7(1.5pt)DSS scheme. Let p = 787, q = 131, d = 57 and e0=5. Find values of e1 and e2. Choose r = 17.
1) Find the values of S1 and S2 if h(M) = 100.
2) Suppose the receiver receives (h(M), S1,S2) = (120, 57, 116). How to verify the signature(show all the intermediate results)?
Note: the signature has nothing to do with the signature created in a)

8(0.5pt). In the Diifie-Hellman protocol, g = 11, p = 983.
a) Suppose Alice's private key is 45 and Bob's private key is 27, what are their public keys, respectively?
b) How does Alice calculate the shared key?
c) How does Bob calculate the shared key?