TNE30024

Deploying Secure Engineering Applications Online

Tutorial 1

Symmetric Key Cryptography

Questions

1. Use the one-time-pad 1010011000 to encrypt and decrypt the message 1111011001

2. The following S-Box (S_1 from the DES standard) maps a six bit input to a four bit output. What will be the output of this box when presented with an input of 7. (All values are base 10.)

Row / Column	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

3. Consider the following simplified block encryption scheme:

   Plaintext is encrypted a byte at a time using the following steps:

   - Step 1.
     - The plain text is expanded to 12 bits by duplicating the first and last two bits (ie, abcdefgh becomes aabbcdefgghh
   - Step 2.
     - A 12 bit sub key is XORed with the expanded text from step 1
   - Step 3.
     - The bit sequence from step 2 is split into two 6 bit sequences and fed into the following two S-BOXes
   - Step 4.
     - The output of the S-BOXes is concatenated and fed through a permutation process that reverses the bit sequence order

   What is the output for a plaintext input of 1001 0100 and a 12 bit sub-key of 1001 0011 1010?

S1		**Middle four bits**															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110
	01	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000
	10	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000
	11	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101

S2		**Middle four bits**															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110
	01	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000
	10	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000
	11	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101

Public Key Cryptography

Questions

4. Bob wishes to send a message to Alice. He wants to encrypt it and digitally sign it using public key encryption.
    a. Which key will Bob use to encrypt the message?
    b. Which key will Bob use to sign the message?
    c. Which key will Alice use to decrypt the message?
    d. Which key will Alice use to validate the digital signature?

5. Is the Diffie-Hellman algorithm a public key encryption algorithm? If not, what is it?

6. 133 is the product of two primes. What are they?

7. RSA and Diffie-Hellman can generate very large numbers that require their modulus to be calculated. Fortunately, modulo arithmetic is associative and commutative. That is:

   $a^{p+q+r} \bmod N = (a^p \bmod N)\ (a^q \bmod N)\ (a^r \bmod N) \bmod N$

   For example

   $3^6 \bmod 5 = (3^2 \bmod 5)\ (3^2 \bmod 5)\ (3^2 \bmod 5) \bmod 5$

   $= (9 \bmod 5)(9 \bmod 5)(9 \bmod 5) \bmod 5$

   $= 4^3 \bmod 5 = 64 \bmod 5 = 4$

   Try this approach with 5^5 mod 23

8. What key do Alice and Bob come to agree upon using the Diffie-Hellman algorithm using the following values?

   Alice chooses a = 3, Bob chooses b = 4, p = 17 and g = 3.

9. The following is a public/private key pair.

   [3,33] and [7,33]

   Use the keys and RSA to encrypt and decrypt‘2’.

10. Generate a public / private key using the prime numbers 3 and 11.