Midterm: Part I

Note

This is a closed-book exam. Part I contains five problems, each accounting for 10 points.

Problems

1. Two keys are inverses if encrypting with one is the same as decrypting with the other. A key is called a *weak key* if it equals its own inverse. DES has four weak keys. The two keys with all ones and all zeros (assuming an even parity) are obviously weak. Please find the other two weak keys. Show the steps of your calculation.

2. (a) For the AES algorithm, how can the multiplication of two bytes (with $x^8+x^4+x^3+x+1$ as the irreducible polynomial modulus) be implemented in terms of shift and bitwise XOR operations? What is the result of (0111 0110)·(0000 0101)? Show the steps of your calculation.
(b) What is the value of $(0110\ 1011)^{-1}$? Show the steps of your calculation.

3. (a) Describe how a typical stream cipher works (e.g., by giving an architectural overview).
(b) What RC4 key value will make the state vector S remain the same as its initial value after initial permutation? Please explain.

```
/* Initialization of S and T*/
for i = 0 to 255 do
    S[i] = i;
    T[i] = K[i mod keylen];

/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i],S[j]);
```

4. Link encryption and end-to-end encryption are the two major alternatives when one considers the placement of encryption function. Please describe how they operate and then compare the two approaches.

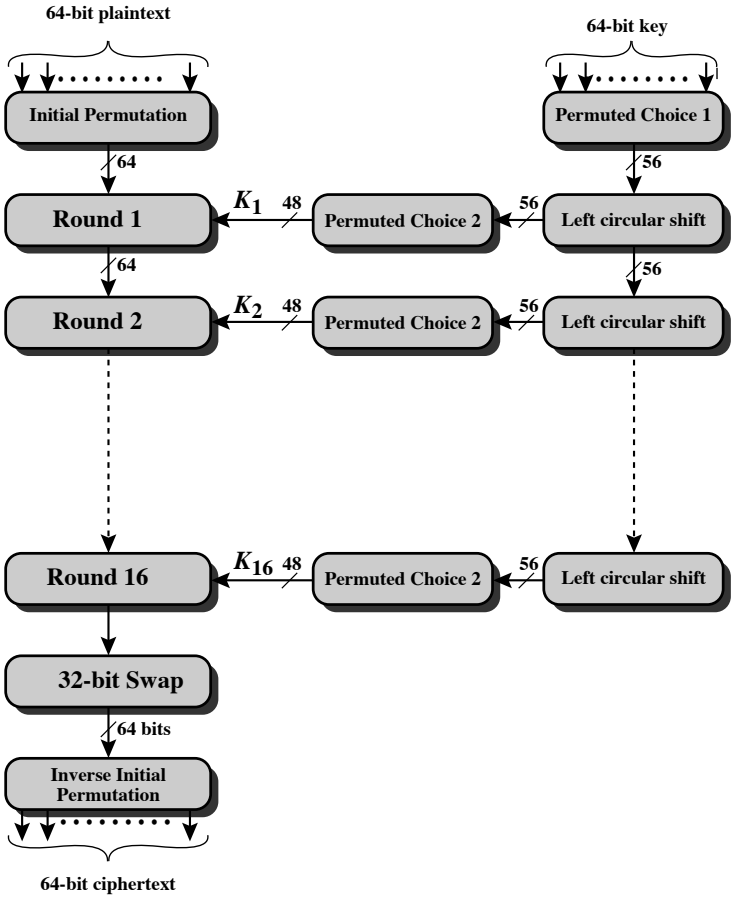
5. Below is a simple authentication protocol that has been studied in the literature. It relies on a trusted third party C that shares a (distinct) secret key with each principle in the system. The key shared between C and a principle P is denoted K_P. $\{M\}_K$ denotes a message containing the plaintext M encrypted with the key K. A nonce is essentially some information that has never appeared before (at the time when the nonce is generated). Please explain why Q can be certain after step (6) that (assuming there is only one session of this protocol running) it was really P who sent the message "I am P".

$$
\begin{array}{lll}
(1) & P \to Q & : \text{"I am } P\text{"} \\
(2) & Q & : \text{generate nonce } n \\
(3) & Q \to P & : n \\
(4) & P \to Q & : \{n\}_{K_P} \\
(5) & Q \to C & : \{P, \{n\}_{K_P}\}_{K_Q} \\
(6) & C \to Q & : \{n\}_{K_Q}
\end{array}
$$

Note: the protocol above is in fact incorrect when there can be multiple sessions running simultaneously.

Appendix

- Some diagrams for DES:

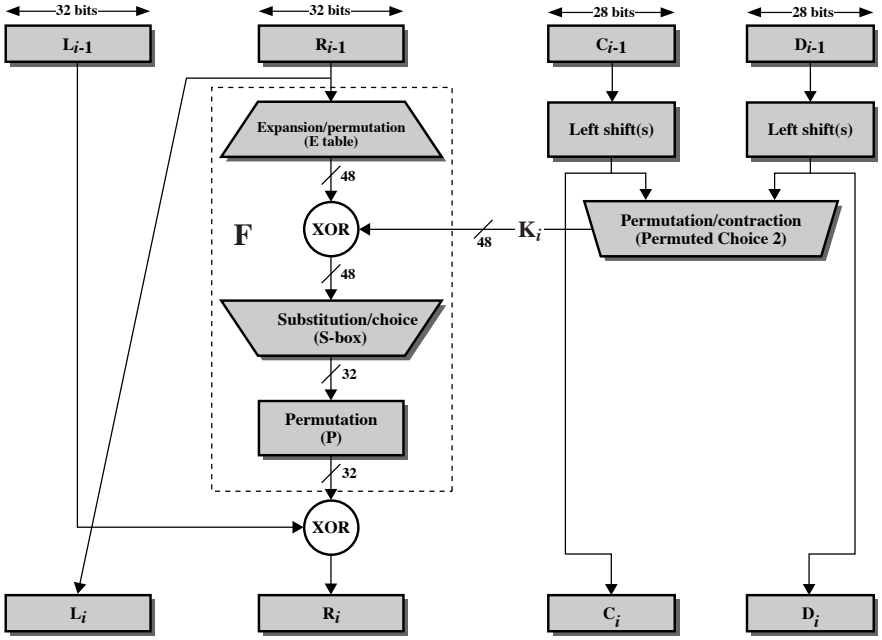


(a) Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4



- The extended Euclid's algorithm for polynomials is as follows.

EXTENDED EUCLID$(m(x), b(x))$:

1. $[A_1(x), A_2(x), A_3(x)] \leftarrow [1, 0, m(x)]; [B_1(x), B_2(x), B_3(x)] \leftarrow [0, 1, b(x)]$
2. if $B_3(x) = 0$ then return $A_3(x) = \gcd(m(x), b(x))$; no inverse
3. if $B_3(x) = 1$ then return $A_3(x) = \gcd(m(x), b(x)); B_2(x) = b^{-1}(x) \pmod{m(x)}$
4. $Q(x) =$ the quotient of $A_3(x)/B_3(x)$
5. $[T_1(x), T_2(x), T_3(x)] \leftarrow [A_1(x) - Q(x)B_1(x), A_2(x) - Q(x)B_2(x), A_3(x) - Q(x)B_3(x)]$
6. $[A_1(x), A_2(x), A_3(x)] \leftarrow [B_1(x), B_2(x), B_3(x)]$
7. $[B_1(x), B_2(x), B_3(x)] \leftarrow [T_1(x), T_2(x), T_3(x)]$
8. goto 2