

b) polyalphabetic cipher

c) one-time pad cipher

3. (5) Encrypt the following plaintext message using a Vigenere cipher with key (2, 1, 4):

HIMOM

4. (5) Arrange the following 16 consecutive bytes of plaintext , expressed in hex, into the state matrix used by AES. Then show the results of rotating this state as specified for one round of processing (do not do any S-box processing).

99 88 77 66 11 22 33 44 AA BB CC DD FF EE 11 00

5. (5) Given the following single column of the state, show the results of of table lookup in the MixColumn table (but do not combine these results using MixColumn processing).

00

44

AA

DD

6. (5) Assume a cryptographic algorithm in which the performance for the good guys grows linearly with the length of the key, and for which the only way to break it is a brute-force attack of trying all possible keys. Suppose performance for the good guys is acceptable (i.e., encrypt/decrypt is not a performance bottleneck) at a certain key size. Then suppose advances in technology make computers twice as fast. Given both good and bad guys get faster computers, does this advance work to the advantage of the good guys, the bad guys, or neither? Explain in a sentence or two.

7. (7.5) In general, will a known cipher consisting of a permutation, a non-linear substitution (involving a key), and another permutation be easier or harder to break than a known cipher consisting of a non-linear substitution (involving a key), a permutation, and another non-linear substitution (involving a key)? Explain your answer in a sentence or two.

8. (7.5) Suppose the input to the function f of one DES round is the 32-bit value
01110111 11001100 00010001 10111011

and the 48-bit key value is:

10101010 01010101 00000000 11111111 10101010 01010101

What is the output of S-box S1 for this input? Show the steps of your computation. You do not need to compute any values except those necessary to compute the output of S1.

9. (7.5) Given the following results of table lookup in the MixColumn table, show the results of combining or mixing these columns as specified for MixColumn. You need only show the expressions, using the appropriate input values. You don't need to actually show the results of evaluating these expressions.

col1	col2	col3	col4
22	88	77	66
33	FF	AA	99
44	BB	CC	DD
55	EE	11	00

10. (7.5) Suppose the input to one round of AES *key* processing was

55	88	77	66
44	FF	AA	99
33	BB	CC	DD
22	EE	11	00

Show the first and second columns of the next round key that is produced. (You don't need to compute the result of the XOR - just show the values that must be XORed together).

11. (7.5) Which processing in the AES cipher accomplishes confusion? Which processing accomplishes diffusion? Explain your answer.

12. (7.5) Given the following plaintext input and ciphertext output produced by a Hill cipher, determine and show the key K . (For convenience, both the letters, and their corresponding numerical position in the upper case alphabet, are shown):

BEDCFH produces **JWRQGT**

or

[1 4 3 2 5 7] produces [9 22 17 16 6 19]

THE FOLLOWING MAY BE SUBSTITUTED FOR ANY OTHER PROBLEM WITH EQUIVALENT NUMBER OF POINTS. SIMPLY ANSWER THE PROBLEM, IF YOU WISH, AND WE WILL DROP THE PROBLEM WITH THE LOWEST SCORE.

13. (7.5) Why is each DES semi-weak key the inverse of another semi-weak key? (Note: "inverse" means "A weak or semi-weak key occurs if there is another key that generates an identical key schedule, but in the reverse order") You can answer this question for two specific semi-weak keys if you wish.