Due Feb 19, 2024 (Monday) at midnight

Note: 10 questions in total for everyone! please read the questions carefully – 471 and 571 have different set of questions to complete. There is also a bonus question in the end for extra credit.

For undergraduate students (ECE471):
Problem 2.13 from Stinson's book (attached below).
Problems 4.2, 4.7, 6.6, 7.4 from textbook;
Additional questions 1-5 (attached below).

For graduate students (ECE571):
Problems 2.3 and 2.13 from Stinson's book attached below.
Problems 4.5, 6.6, 7.4 from textbook;
Additional questions 1-5 (attached below).

Questions from Stinson's book:

2.3 (a) Prove that the *Affine Cipher* achieves perfect secrecy if every key is used with equal probability $1/312$.

(b) More generally, suppose we are given a probability distribution on the set

$$\{a \in \mathbb{Z}_{26} : \gcd(a, 26) = 1\}.$$

Suppose that every key (a, b) for the *Affine Cipher* is used with probability $\mathbf{Pr}[a]/26$. Prove that the *Affine Cipher* achieves perfect secrecy when this probability distribution is defined on the keyspace.

2.13 Consider a cryptosystem in which $\mathcal{P} = \{a, b, c\}$, $\mathcal{K} = \{K_1, K_2, K_3\}$ and $\mathcal{C} = \{1, 2, 3, 4\}$. Suppose the encryption matrix is as follows:

	a	b	c
K_1	1	2	3
K_2	2	3	4
K_3	3	4	1

Given that keys are chosen equiprobably, and the plaintext probability distribution is $\mathbf{Pr}[a] = 1/2$, $\mathbf{Pr}[b] = 1/3$, $\mathbf{Pr}[c] = 1/6$,

Does this cryptosystem have perfect secrecy?

Additional questions for all students (problems 1-5):

Problem 1:
If the useful life of DES was about 20 years (1977-1999), how long do you predict the useful life of AES (128-bits key) to be? Justify your answer. (Hint: you may need to consider the Moore's Law (Google it) in order to answer this problem.)

Problem 2: What is the output of the first round of DES when the plaintext and the key are both all zeros? What if the plaintext and the key are all ones? (Complete details of each DES round can be found in the textbook appendix S, or here: http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm)

Problem 3: An important property which makes DES secure is that the S-boxes are nonlinear. Verify the nonlinearity of the S-boxes by computing the output of box S_1, for three pairs of inputs. Then show that

$$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$$

for

a. $x_1 = 000000$, $x_2 = 000001$
b. $x_1 = 111111$, $x_2 = 100000$
c. $x_1 = 101010$, $x_2 = 010101$

The first S-Box is shown below:

Input bits 1 and 6 ↓	Input bits 2 thru 5															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Problem 4: Assume that bit 57 of a 64 plaintext block is 1 with all other bits equal to zero. Let the key be all zeros.

a. How many S-boxes get different inputs compared to the case of an all-zero plaintext, in the first round of DES?
b. What is the number of output bits which are different compared to the input after the first round?
c. How many output bits have actually changed after the first round compared to the case of an all-zero plaintext (consider only one round). Does DES exhibit the *avalanche effect* (small changes in the plaintext yield significant changes in the ciphertext)?

Do not forget to apply the initial permutation on the plaintext before passing it through the DES round.

Problem 5: Consider the following alternative method of encrypting a message. To encrypt a message, use the algorithm for doing a CBC decrypt. To decrypt a message, use the algorithm for doing a CBC encrypt. Would this work? What are the security implications of this, if any, as contrasted with the "normal" CBC?

Bonus Question for all (10% extra points):

Problem 6: Find keys K such that

$$DES_K(DES_K(x)) = x, \forall x$$

Such a key is sometimes called a "weak" key. How many weak keys can you find? To solve this problem you need to look up the exact key schedule generation algorithm for DES. For details refer to http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm (Show your work or you will receive zero credit!)