Name:

Login:
**Question 1: (15 points)**

When grading assignment 1 part II, one of you have the following observation:

If the original document is an English text, then it must contain spaces (SP).

The ASCII representation of SP is 0x20 while A-Z is 0x41-0x132 and a-z is 0x132-0x172.

Thus the XOR of “SP” with an *upper case* char produces *lower case* char, e.g., \( SP \ XOR \ A \rightarrow a \) and vice versa.

Describe how to utilize this fact in finding the encryption key?

**Solution:**
**Question 2: (10 points)**

Assume we have the following encryption scheme:

(I) *Caesar-based cipher*: Divide the string into 2 bits long blocks and replace each block with another block K positions away with wrap around.

(II) *Monoalphabetic-based cipher*: Arbitrary map one 2 bits block with another block.

How much computational effort Trudy has to perform to find the encryption key for both I and II using brute-force attack?

**Solution:**

I.

II.
Question 3: (20 points)

In this question, we will use the following notations:

- P and V are the Public and its corresponding private keys.
- K is a symmetric Key.
- M is a Message and C is the corresponding cipher
- $K \{M\}$: message M is encrypted with K.
- $K [M]$: message M is decrypted with K.
- $\{M\}_P$: message M is encrypted/verified with P.
- $[M]_V$: message M is decrypted/signed with V.
- $H(M)$: the hash of message M.

Assume that Bob and Alice agree on a shared secret $K$ and $e_A/d_A \ (e_B/d_B)$ are the public/private key pair of Alice (Bob).

Bob may authenticate himself to Alice using any of the following methods:

1. Bob sends Alice: $C = K\{K\}$
2. Bob sends Alice: $C = \{K\}e_A$
3. Bob sends Alice: $C = H(K)$
4. Bob sends Alice: $C = \{K\}d_B$

In each method, describe what Alice should do when she receives C in order to authenticate Bob.
**Solution:**

- 1.
- 2.
- 3.
- 4.

Which of these 4 alternatives have a serious security risk and why?
Question 4: (10 points)

I. In DES, a key K is called a weak key if for any message m: K(m) = K[K(m)].

What is the result of:

1. K(K(m))
2. K[K(m)]
3. K[K(m)]
4. K[K(m)]

II. Repeat if K is a non-weak key.

Solution:

I. Weak:

1. K(K(m))
2. K[K(m)]
3. K[K(m)]
4. K[K(m)]

II. Non-Weak:

1. K(K(m))
2. K[K(m)]
3. K[K(m)]
4. K[K(m)]
Question 5: (30 points)

Show the result, in HEX, of the first octet of the 1st round to encrypt one data block of all 0s using a key of all 0s using:

1. DES*
2. IDEA
3. AES-128

Solution:

DES:

IDEA:

AES-128:

* Since I have posted only the first 2 S-box in my web page, you may assume that the content of the other missing S-Boxes are all 0s.
Question 6: (15 points)
Is it possible to launch an append attack on MD2 and why?

Solution: