Assignment 1

1. A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: for each plaintext letter p, substitute the ciphertext letter C:

$$C = E([a,b], p) = (ap + b) \bmod 26$$

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a=2 and b=3, then $E([a,b],0) = E([a,b],13) = 3$.

   a) Are there any limitations on the value of b ? Explain why or why not.
   b) Determine which values of a are not allowed.
   c) Provide a general statement of which values of a are and are not allowed. Justify your statement.

2. Decrypt the following ciphertext :

```
JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWE
OGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILE
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX
```

3. Provide a formal definition of the Gen, Enc, and Dec algorithms for the mono-alphabetic substitution cipher.
4. Show that the shift, Substitution, and Vigenere ciphers are all trivial to break using a chosen-plaintext attack. How much chosen plaintext is needed to recover the key for each of the ciphers?
5. Encrypt the message “meet me at the usual place at ten rather than eight oclock” using the Hill cipher with the key

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$

   a) Show your calculations and the result.
   b) Show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext.

6. Prove or refute: An encryption scheme with message space M is perfectly secret if and only if for every probability distribution over M and every $c_0, c_1 \in C$ we have $\Pr[C = c_0] = \Pr[C = c_1]$.

7. For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

a) The message space is $M = \{0,\ldots,4\}$. Algorithm Gen chooses a uniform key from the key space $\{0,\ldots,5\}$. $Enc_k(m)$ returns $[k + m \bmod 5]$, and $Dec_k(c)$ returns $[c - k \bmod 5]$.

b) The message space is $M = \left\{ m \in \{0,1\}^L \mid \textit{the last bit of } m \textit{ is } 0 \right\}$. *Gen* chooses a uniform key from $\{0,1\}^{L-1}$. $Enc_k(m)$ returns ciphertext $m \oplus (k \| 0)$, and $Dec_k(c)$ returns $c \oplus (k \| 0)$.

8. Let Π denote the Vigenere cipher where the message space consists of all 3-character strings (over the English alphabet), and the key is generated by first choosing the period t uniformly from $\{1,2,3\}$ and then letting the key be a uniform string of length t.

a) Define A as follows: A outputs $m_0 = aab$ and $m_1 = abb$. When given a ciphertext c, it outputs 0 if the first character of c is the same as the second character of c, and outputs 1 otherwise. Compute $\Pr\left[\Pr ivK^{eav}_{A,\Pi} = 1\right]$.

b) Construct and analyze an adversary A' for which $\Pr\left[\Pr ivK^{eav}_{A',\Pi} = 1\right]$ is greater than your answer from part (a).

Note:

1. Due date: Sunday, October 7, 2018, at 23:59. Send your assignment to the following email: 2821785913@qq.com
2. Assignment should be named by UNo+Name+A1.docx/doc/pdf.
3. Penalty for late submission: 15% of the total marks for every day after the deadline.
4. Answer All 8 questions.