**ECE568: Assignment2**

Name: Chuanrui Li; Student Number: 1000010846

**Basic Ciphers**

**Part1:**

Shift cipher has 47 possible keys and substitution cipher has P(n = 47, r = 47) unique possible keys, so the answer is about 2.586232415 E+59 which is equal to 47!.

For the polyalphabetic ciphers with period 3, it will have has (47!)^3 possible keys because every period-3-key is a combination of three different keys.

The polyalphabetic cipher is considered more secure. Attacker needs to take an extra step to guess the period. The bigger period that the key has, the harder it can be guessed, because the larger period causes more complex encryption and mapping.

**Part2:**

In general, polyalphabetic chipper is better than shifting and substitution encryption, because polyalphabetic can create a set of n mapping, which is hard for attackers to guess the plaintext using cipher text. It is also based on the content that needs to be encrypted. In worst case, all three encryption methods will same effect for certain plaintext. For the shifting base and substitution base encryption, one way may be better than another in the following case.

If the content has partial repeating pattern, shifting base is better. For example, plaintext is “1123445” and shifts right by 2, so the same 1 and 4 in plaintext will match different number in cipher text. Compared with substitution, shifting encryption is better in this case.

If the content has same number, substitution base is better. For example, plaintext is “111111”. Substitution base is better because shifting will not change the plaintext.

**Key Exchange**

**Part1:**

Mallory can discover the secret number x, y by solving the discrete logs for P and Q, respectively.

**Part2:**

x = **4**, for P = (g^x) mod n, P = 4, g = 5 and n = 23

**Part3:**

y = **17**, for Q = (g^y) mod n, Q = 15, g = 5 and n = 23

**Part4:** Secret key = [g^(xy)] mod n **=** [5^(4\*17)] mod 23 = 2

**SSL**

**Part1:**

If there is an error in the message or attacker changes the message content, the entire message will be resent again. However, if we send 4KB fragments one by one, we only need to resend the fragment with error not entire message. Also, some network protocols may not be able to transfer a large file in one package, resulting in a failure.

**Part2:**

There will be more bytes that need to be transferred, which costs more time to transmit a file. As a result, it becomes less efficiency as messages are longer.

**Part3:**

Attacker can do the reordering and replay attacks, or even delete the message in the middle of transmission.

**Part4:**

Attacker can do spoofing attack and break the integrity rule. For example, he can change the data in the package during the transmission. Also, receiver does not know the sender without MAC, breaking the authenticity rule, too.

**Part5 (not required in assignment):**

Attacker can break confidentiality rule. For example, he can know the content of message and MAC value for the message

**Trust**

**Part1:**

The purpose of “{k} Kas” is to create a secret counter encrypted by the shared key between Alice and Samantha, which can avoid additional verification steps between them. Then Alice can check the counter k directly, so Samantha does not have to be online all the time.

Since k is unique, Alice can decrypt the message to track the numbers and ignore the duplicated k values, which prevents replay attack.

Kas is used to protect data integrity and confidentiality. Because only Alice and Samantha have the right to see the k, so attacker cannot access the data. This can also help Alice know that Samantha is the sender of the package.

**Part2:**

Since k is unique, this will prevent the replay attack. To be more specific, Samantha generates the unique counter, k, for Bob and asks him to grant bridge service for Victor. If attacker sits in the middle and does the replay attack, he will not get the right to join the network later because Bob will ignore the message.

First, Nas tells Bob and Samantha that Alice manages to recruit Victor to join the Tor network. If Victor does some malicious actions within the network later, Bob’s IP will be on blacklist. However, Samantha, administrator of network, will know that Alice recruited attacker by mistake not Bob. Second, Nas is also used as a verification code in the last step between Bob and Samanth, which mean that Bob has successfully received Samantha’s message.