Name: Terry Liang
EID: twl378
CS Login: tliang
Email: liang810612@hotmail.com

Assignment 3

Lecture 34

1. Because we know we can transmit at an average rate of (C/h) –e. The best transmission would be C/h. And there is no more room left in the channel, so you cannot do greater than average.
2. Increasing the redundancy of the coding scheme can make sure that the information can finally make through.

Lecture 35

1. H = - (log1/10) = 3.32
2. Figuring out the letters following by other letters are difficult, and it requires sophisticated model and still only get an estimate.
3. Zero-order: we assume that all characters are equally likely.
   First-order: we assume some symbols occur much more frequently than others.
   Second-order: we assume some letters follow other letters frequently and only assuming two letters.
   Third-order: it is the same as second-order but with assumption on three letters.

Lecture 36

1. Because you do not know what thing will happen.
2. Because if someone already know the probabilities of some event, the entropy will be zero and that means there is no uncertainty.
3. Entropy can be used to measure the amount of redundancy in the encoding.
   If the information content of a message is equal to the length of the encoded message, there is no redundancy.

Lecture 37

1. This message has a big possibility that it's a direction to where the treasure is. There is many redundancies in this encryption. However, we do not know what the underlying language is.
2. The key selects a specific algorithm from the family of algorithms.

3. The encrypting message should be preserved, so that it would not be destroyed or created during the process of decrypt.
4. The redundancy is the enemy of secure encryption because it provides leverage to the attacker.

Lecture 38

1. {P}
2. {{{{P}Ke}Ke}Kd}
3. The pattern of the language can be a clue for the cryptanalyst to decrypt the message.
4. If the cryptanalyst knows that properties of the language, it could deduce the code using like, the redundancy of the language.

Lecture 39

1. Because the time and space needed to decrypt might be too large to break.
2. Because if we do a linear search, on average, we find the right one in the middle of the process. That is why we need 2^n -1 operations.
3. Substitution and transportation can bring the Confusion and Diffusion to the enemy.
4. Confusion is transforming information in plaintext so that an interceptor cannot readily extract it.
   Diffusion is spreading the information from a region of plaintext widely over the cipher text.
5. I think diffusion is a better strategy because people can still store the data fully with enough time if there is confusion in the plaintext.

Lecture 40

1. Monoalphabetic cipher is replacing symbols uniformly by others.
   Polyaphabetic substitution means that substitution varies according to the position in the text.
2. The range between two alphabets.
3. There are only finite number of table and depends on size of k.
4. 2
5. 26
6. No, it is easy to break.
7. Line up two strings and look up the the Vigenere Tableau to find the corresponding letter.

Lecture 41

1. Each x, y, and y has 26 possible choices.
2. Because it is a simple substitution and y would have to be the same alphabet.
3. I do not think so because there are so many examples in the real world that has already proven the point.

Lecture 42

1. Every possible plaintext could be the pre-image of that ciphertext under a plausible key.
2. If we know the number of keys, we can eliminate many possible plaintexts.
3. The problem is about how to the sender and receiver agree on a secret that they can use in the algorithm. If they already have a secure channel, they do not need a key. If they don't, how are they going to distribute to the other side.

Lecture 43

1. The transposition does not replace the characters, we can still use the letter frequencies preserved in the ciphertetxt.

Lecture 44

1. It is a symmetric algorithm.
2. Key distribution is how to convey keys to those who need them to establish secure communication
   Key management is given a large number of keys, how do we preserve their safety and make them available as needed.
3. No. Because there is a K-1 that would only work to decrypt.
4. They are not comparable, it depends on where we want to use it.

Lecture 45

1. Because it has a higher diffusion and immunity to tampering.
2. People can make some changes that would significantly affect the meaning of the plaintext without being notices.
3. It allows the chaining together of different services without exposing the data to each of those services.

Lecture 46

1. subBytes, shiftRows, mixColumns, addRoundKey. The key is initially expanded in a recursive process into r+ 1 128 bit keys. And it uses 1-, 12 ,14 rounds for keys of 128, 192 , 258 bits

2. subBytes, shiftRows, mixColumns, addRoundKey. It prelacee byte by the value stored at that location and shift rows left or right with different bytes.
3. Because the subkeys are used in a reverse order and each step is inverted, and the first and last rounds are slightly different.
4. They key is arranged as a 4 * n array of bytes. And it is a recursive process into r +1 128-bit keys where r is the number of rounds.
5. For a higher security reason.

Lecture 47

1. It leaves too much regularity in the ciphertext.
2. We can use CBC to randomize blocks before they're encrypted.
3. An attacker able to observe changes to ciphertext over time will be able to spot the first block that changed.
4. It uses encryption algorithms to generate random appearing streams of bits in reproducible fashion.

Lecture 48

1. the secret key
2. It is easy to computer, but hard to invert.
3. There is no need for a safe channel.
4. {P} K-1
5. Asymmetric encryption may take 10,000 times as long to perform as a symmetric encryption

Lecture 49

1. Yes. Either key can be used to encrypt or decrypt.
2. The prime number provide the difficulty to factor out large number.
3. No
4. Only A has the key to decrypt.
5. because anyone can have A's public key
6. because A has B's private keys
7. Anyone can use B's public key to decrypt.
8. B will need to pairs of keys: one for privacy and one for authenticity.

Lecture 50

1. Because it just converts variable-sized text into a small datum, and its fixed size.
2. The argument might equal in strong collision, while it's not the case in weak collision.
3. Preimage has one argument, and second preimage has two.
4. 1.25 * 2 ^64

5. 1.25 & 2 ^ 80
6. In a secure communications system, the correct transmission of messages may override confidentiality concerns.
7. It binds the bytes of a file together that makes any alterations to the file apparent.
8. The hash function can assure confidentiality and the private key can assure integrity.

Lecture 51

1. No. Because we do not know about the confidentiality.
2. No. Because we need to make sure R is the one decrypt message first.
3. Yes.
4. It requires both confidentiality and authentication, so the information can be sent in a safe environment.

Lecture 52

1. It would still be secure because they do not have information on b.
2. It would still be secure because they do not know about p, g, b.
3. It is secure because they do not know about p, g , a.