Lena Ko
EID: lk5399
CS: lk5399
ko.lena92@gmail.com

Lecture 34

1. C is the amount of bits per second that can be transmitted while the entropy of a language is (bits per symbol). A perfect channel transmits at C/h-e which is the greatest rate.

2. If entropy is less than the capacity, there exists a coding that the output of the source can be transmitted over a channel with an arbitrarily small frequency of errors. If a channel can handle message traffic, then it is possible to transmit with a small error rate.

Lecture 35

1. h= -log 1/10

2. Computing entropy of a natural language is difficult because it requires sophisticated models and you can probably only get an estimate.

3. zero order: assumes all characters are all equal
   first order model: some symbols occur more frequently than others but all symbols are independent
   third higher order: Some letters follow others frequently and others don't at all

Lecture 36

1. It is impossible to calculate every situation that could happen.

2. The message depends not he state of knowledge of the receiver because the observer may already know the answer. The way a message is interpreted depending on what the observer already knows.

3. Entropy can be used to measure the amount of redundancy in the encoding. If information content of a message is equal to the length of the encoded message, there is no redundancy.

Lecture 37

1.The text is seems to be the location of buried treasure. There seems to be much redundancy so a symbol could represent a letter or directions. Some letters in english may be more prevalent. It may be a simple algorithm because it was done by a pirate.

2. A key is optional because there may be a use of keys, one key, or no key.

3. Hopefully, the information is preserved, not destroyed.

4. Redundancy means regularities of the number of the same symbol, so the attacker can use those to decrypt the message.

Lecture 38

1. P

2. P

3. Recognizing patterns may give some clues about an algorithm to decrypt a cipher text.

4. Properties of a language show frequencies and probabilities of symbols in languages.

Lecture 39

1. It is breakable because all keys can by tried systematically, but it is not feasible because it could take a long time.

2. As n gets bigger, the time of search gets bigger.

3. They are used in almost all modern commercial symmetric ciphers and are very powerful in combination.

4. Confusion is transforming information in plaintext so that an interceptor cannot readily extract it. Diffusion means moving information for a region of plaintext widely over the cipher text.

5. Both should be used for encryption. Confusion is better for substitution and diffusion is better for transfusion.

Lecture 40

1. Monoalphabetic cipher means each letter is substituted by the same letter -uniformly. Polyalphabetic substitution means you use different letters for each letter.

2. However you specify the mapping such as a table.

3. k! would be trying all mappings possible.

4. The caesar cipher key is how many positions you shift.

5. The keyspace is the 26 letters.

6. No.

7. Find the cipher text letter in the table and find the corresponding letters on the row and column.

Lecture 41

1. There are 26 different letters with a length of 3 so that is 26^3.

2. Now each letter has to be different and two letters are the same.

3. I'm not sure. I guess it could be possible under the right

circumstances.

Lecture 42

1. Even by knowing the encryption algorithm and the cipher text, nothing would be gained. You can't remove any of the possibilities, so no reduction of the search space is possible.

2.The key has to be random because if you knew something about the key, you could eliminate some of the plaintext.

3. How do you distribute the key securely and if they have a secure channel why don't they just not encrypt it?

Lecture 43

1. The downside to using transposition for encryption is that it preserves letter frequencies so it can be easily seen to be a transposition encryption.

Lecture 44.

1. A one time pad is a symmetric encryption.

2. Key distribution is deciding how to keep all the keys straight and which one to use. Key management is about preserving the safety of the key.

3.No, decrypting requires Ks-1, the decrypting key.

4. Both encryptions have two very different approaches so it depends on the context which is better.

Lecture 45

1. Most modern symmetric encryptions may be block ciphers because they are non malleable and less susceptibility and less diffusion.

2. Malleability means that changes to the cipher text produce meaningful changes in the plaintext.

3. Hormomorphic encryption is where a specific algebraic operation performed on the plaintext is equivalent to another algebraic operation performed on the cipher text. The are malleable by design. They can create secure voting systems, collision-resistant hash functions, and private information retrieval schemes.

Lecture 46

1. The step that uses confusion in AES is subBytes. Each byte int he array is replaced by another byte from a table of 256 elements. shiftRows shifts down n to the left. addRoundKey XORs the state with a 128 bit round key derived from the origin key K.

2. mixColumns uses both confusion and diffusion. Each column of the state, replace the column by its value multiplied by a fixed 4X4 matrix of integers.

3. Decryption takes longer because you have to multiply by the inverse of the array in the mixColumns array.

4. A 128 block is arranged as a 4x4 array of bytes called the state which is then modified in place in each round.

5. Adding rounds adds more modification, therefore making it more difficult to decrypt.

Lecture 47

1. Similar blocks in the plaintext will have similar blocks in the cipher text, yielding a similar image/plaintext.

2. You can fix this problem with randomizing blocks before they are encrypted by using CBC where you XOR each successive plaintext

block with the previous cipher text block and then encrypt it.

3. Weaknesses of CBC include observed changes where an attacker is able to observe changes to the cipher text over time will be able to spot the first block the text changed. Another weakness is a content leak where an attacker can find two identical cipher text blocks he can derive information about two plaintext blocks.

4. Block encryption modes generate cipher text that stores the message in encrypted but recoverable form. Key stream generation modes- cipher is used more as a pseudorandom number generator. The result is a key stream that can be used as in one- time-pad. Decryption uses the same key stream.

Lecture 48

1. The decrypt key must be kept secret.

2.The public key system is easily computed, but difficult to invert without information.

3. In public key cryptography, the key distribution of public keys is done through public key servers. When a person creates a key-pair, one key is private and the other is public uploaded on a server.

4. Decrypt plaintext

5. Asymmetric encryption is less efficient than symmetric. It may take up to 10,000 times longer to perform.

Lecture 49

1. You can uses either key because of the symmetric fashion, but new keys would not work.

2. RSA is based on factoring large prime numbers.

3.Yes, RSA is breakable

4. They don't have the decryption key.

5. Anyone could have A's public key.

6. Only B has B's private key.

7. Anybody might have B's public key.

8. By using two pairs of keys, one for authentication and one for confidentiality.

Lecture 50

1. You may need to compute it multiple times.

2.Weak collision: a function is weak if given an input m1 it is hard to find m2 that does not equal m1 such that f(m1)=f(m2).Strong collision: it is hard to find two messages m1 and m2 such that f(m1)=f(m2)

3. For pre image, given h, it is hard to find a m such that h=f(m). While second pre image is hard to find a m2 that doesn't equal m1 such that f(m1)=f(m2)

4. 1.25*2^64

5. 1.25*2^80

6. Hash functions are used for integrity, not confidentiality because they bind the bytes of a file together in a way that make alterations to the file apparent.

7. It is binding.

8.B can securely send a message to A using a hash function and storing the value then using RSA to send the message.

Lecture 51

1. No, both public keys are released.

2. Yes, you could do it the other way around.

3. Yes.

4. Confidentiality and authentication; for correct key exchange.

Lecture 52

1. Nothing, only a and b secret numbers need to be kept secret.

2. If a is discovered and p , g , and the message were also known, the eavesdropper could decode Bob's message.

3. If b is discovered and p, g, and the message were also known, the eavesdropper could decode Alice's message.