Name:Cohen Ellis
EID: cce335
CS Login: coel09
Email: coel09@yahoo.com

CS361 Questions: Week 3

The questions marked with a dagger (†) require external research and may be more extensive and time consuming. You don't have to do them for the assignment but, but do them to increase your competency in the class.

Lecture 34

1. Why is it impossible to transmit a signal over a channel at an average rate greater than C/h?

   C/h is the entropy of the information being transferred. Entropy provides a bound on coding efficiency and we can only get lower than the bound, but not higher

2. How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?

   Everything we send would be corrupted because of the noise. If we send multiple times, there is a greater chance that the message would get through.

Lecture 35

1. If we want to transmit a sequence of the digits 0-9. According to the zero order model, what is the entropy of the language?

   H= -(log 1/10)

2. What are reasons why computing the entropy of a natural language is difficult?

   Real life languages are complex and require multiple diagrams.

3. Explain the difference between zero, first, second and third-order models.

   Zero order can be computed when all symbols are equally likely. First order depends on the likelihood of various symbols while second and third depends on the likelihood of a symbol after a given symbol.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

   We do not always know the probabilities and that it depends on many factors like uncertainty and redundancy.

2. Why is the information content of a message relative to the state of knowledge of an observer?

The more knowledge of the observer, the less the uncertainty and information that needs to be passed through.

3. Explain the relationship between entropy and redundancy.

   If we have an efficient entropy or optimal entropy, we can lower the redundancy. Entropy can be used to measure the amount of redundancy.

Lecture 37

1. List your observations along with their relevance to cryptography about Captain Kidd's encrypted message.

   I noticed that the message uses English based characters so we should know the language, and we can find the frequency of the symbols.

2. Explain why a key may be optional for the processes of encryption or decryption.

   A key will help to alleviate the uncertainty of the message.

3. What effect does encrypting a file have on its information content?

   It decreases the amount of redundancy and uses compression, but makes it difficult to decrypt.

4. How can redundancy in the source give clues to the decoding process?

   We can use frequency of certain symbols to guess what they can be translated to.

Lecture 38

1. Rewrite the following in its simplest form: $D(E(D(E(P))))$.

{{P}, E, D}

2. Rewrite the following in its simplest form: $D(E(E(P,K_E),K_E),K_D)$.

   {{{P}Ke}Ke}Kd

3. Why might a cryptanalyst want to recognize patterns in encrypted messages?

   This helps to make for easier decryption.

4. How might properties of language be of use to a cryptanalyst?

   He would be able to recognize patterns in order to break the message and deduce the key.

Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?

   If it is strong it may take years to break.

2. Why, given a small number of plaintext/ciphertext pairs encrypted under key K, can K be recovered by exhausteive search in an expected time on the order of 2^{n-1} operations?

   The keyspace is small so it can be recovered in a small amount of time.

3. Explain why substution and transposition are both important in ciphers.

   We want to confuse and diffuse the reader and using only one method will not work to do both.

4. Explain the difference between confusion and diffusion.

   To confuse we take the symbol and turn it into another so that it is hard to decrypt while diffusion mixes the symbols around.

5. Is confusion or diffusion better for encryption?

   Diffusion is better because it is harder to decrypt.

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substitution?

   Monoalphabetic has the same symbol replaced uniformly while polyalphabetic has the same symbol replaced by different symbols depending on their position.

2. What is the key in a simple substitution cipher?

   The key is a table that exhibits the mapping.

3. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?

   K is the number of different symbols in plaintext, and eventually one of the k symbols is the correct substitution.

4. What is the key in the Caesar Cipher example?

   The key is a table that exhibits the mapping.

5. What is the size of the keyspace in the Caesar Cipher example?

   The size of the keyspace is 26, since that is how many symbols in the alphabet.

6. Is the Caesar Cipher algorithm strong?

   It is not strong.

7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?

   A table that shows the sentence and key, and the position of those symbols in the table is the substituted symbol.

Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide3?

   We assume that xyy are different symbols, so therefore each can be a total of 26 symbols.

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?

   We assume that y is the same symbol, so when x is out of 26 and found, the same symbol for x is not the same symbol for y, and we do not need to find the symbol for the second y.

3. Do you think a perfect cipher is possible? Why or why not?

   Ciphers are created to send hidden information and for someone else to open. It will always need to be read.

Lecture 42

1. Explain why the one-time pad offers perfect encryption.

   Even though we know the cipher, every possible plaintext could be the pre-image of that possible key.

2. Why is it important that the key in a one-time pad be random?

   If the key is not random and we know something about it, we can reduce the search space significantly and it will no longer be a perfect cipher.

3. Explain the key distribution problem.

   The sender and receiver have to send the key, and if they can do it secretly then why do you need the key, but if it is not secure, how do you send the key.

Lecture 43

1. What is a downside to using encryption by transposition?
   It has a greater space complexity, and can cause a delay in the decryption.

Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?

   Asymmetric.

2. Describe the difference between key distribution and key management.

   Key distribution is who gets the key, key management is how to keep them safe once you have passed them out.

3. If someone gets a hold of Ks, can he or she decrypt S's encrypted messages? Why or why not?

   There are different K's to encrypt and decrypt, so they would not be able to decrypt the message.

4. Are symmetric encryption systems or public key systems better?

   Public key systems are better because they make for stronger encryptions.

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?

   With immunity to tampering, no one can change in the middle of decrypting.

2. What is the significance of malleability?

   You can make changes to the ciphertext which can change the overall plaintext. You can change the meaning of the plaintext.

3. What is the significance of homomorphic encryption?

   Theses encryptions are malleable by design.

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?

   subBytes replaces one byte with another

2. Which of the 4 steps in AES uses diffusion and how is it done?

   shiftRows shifts the rows depending on its position.

3. Why does decryption in AES take longer than encryption?

   You have to multiply by a fixed array that takes a lot of time to create.

4. Describe the use of blocks and rounds in AES.

   This way the message is completely encrypted and is not malleable.

5. Why would one want to increase the total number of Rounds in AES?

   That way the encryption could be completely scrambled with a larger message.

Lecture 47

1. What is a disadvantage in using ECB mode?

   If you have identical blocks in the plaintext, the result will be identical ciphertext.

2. How can this flaw be fixed?

   Randomizing the identical blocks.

3. What are potential weaknesses of CBC?

   If someone is watching the encryption, they can see where the changes occur.

4. How is key stream generation different from standard block encryption modes?

   Key stream is used as a random number generator, while standard blocking chains them together.

Lecture 48

1. For public key systems, what must be kept secret in order to ensure secrecy?

   The decryption key.

2. Why are one-way functions critical to public key systems?

   This way you can give out the encryption keys, but keep the private key.

3. How do public key systems largely solve the key distribution problem?

We can still give out the encryption key and it doesn’t matter who reads it, only you can decode it.

4. Simplify the following according to RSA rules: $\{\{\{P\}_{K-1}\}_{K}\}_{K-1}$.

{{P}k}k-1

5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.

   Symmetic algorithms are more efficient and take a shorter time to encrypt than asymmetric.

Lecture 49

1. If one generated new RSA keys and switched the public and private keys would the algorithm still work? Why or why not?

   No because it is public, anyone can decrypt the message.

2. Explain the role of prime numbers in RSA.

3. Is RSA breakable?

   It is breakable if you have both keys.

4. Why can no one intercepting $\{M\}_{K_a}$ read the message?

   They need to have access to the decryption key.

5. Why can't A be sure $\{M\}_{K_a}$ came from B?

   Someone else might have access to B's public key.

6. Why is A sure $\{M\}_{K^{-1}}$ originated with B?

   Only B has access to the private key.

7. How can someone intercepting $\{M\}_{K^{-1}}$ read the message?
   If they have access to both the encryption key and the decryption key.

8. How can B ensure authentication as well as confidentiality when sending a message to A?

Only B has access to the private key and just has to make sure that A has the public key.

Lecture 50

1. Why is it necessary for a hash function to be easy to compute for any given data?

2. What is the key difference between strong and weak collision resistance of a hash function.

   Strong means that it is difficult to find the same hash function for different sets of data, and weak means that it is easy to find this functions.

3. What is the difference between pre-image resistance and second pre-image resistance?

   Pre-image is if the hash function should not be the same as the original while second means that two of the same functions should not have the same hash function.

4. What are the implications of the birthday attack on a 128 bit hash value?

   There will be about 14 collisions.

5. What are the implications of the birthday attack on a 160 bit hash value?

   There will be about 16 collisions.

6. Why aren't cryptographic hash functions used for confidentiality?

   We want to make sure that the message sent is the same message received more than who it is who saw it.

7. What attribute of cryptographic hash functions ensures that message M is bound to $H(M)$, and therefore tamper-resistant?

   It binds the bytes of the file together and makes a seal.

8. Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?

   B can send the file to A which can change whenever it is accessed.

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following message: $\{\{K\}_{KS^{-1}}\}_{K^{-1}}$? Why or why not?

Any person can see the message and be able to decrypt using the public key to decrypt.

2. In the third attempt at key exchange on slide 5, could S have done the encryptions in the other order? Why or why not?

   No because you encrypt with the private key, others can decrypt with the public key.

3. Is $\{\{\{K\}_{KS^{-1}}\}_{K_R}\}_{K_S}$equivalent to$\{\{K\}_{K_S^{-1}}\}_{K_R}$?

   Yes.

4. What are the requirements of key exchange and why?

   We need to have access to either the public or private keys.

Lecture 52

1. What would happen if g, p and $g^a \text{mod} p$ were known by an eavesdropper listening in on a Diffie-Hellman exchange?

   They would need to know b and a, so they would not be able to know the final number.

2. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?

   The eavesdropper would still need to know b.

3. What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?

   If they knew the formula, they could figure out the number.