CS361 Questions: Week 3

Daniel Ricaud

UTeid: dr25237

CSid: dr25237

Thequestionsmarkedwitha dagger(†) requireexternalresearch and maybemore 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?

Because you cant transmit a signal faster than the channel will even allow you too.

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

Because it helps separate the message from the noise.

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?

3.32

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

It requires complex models.

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

Every order adds a new level of grouping. For example, zero assumes every letter in the alphabet is equally likely to occur, first takes the letter probability into account, second takes probabilities of groups of letters into account, and finally third takes into account the probability of entire words.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

Because the entropy is different for different people.

Because if the observer already knows the information contained in the message then the entropy is zero since it contains no useful information.

2. Explain the relationship between entropy and redundancy.

The closer you get to achieving entropy the less redundancy you have.

Lecture 37

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

It seems difficult to decrypt a random message like that because you don't even know how many symbols you have to choose from.s

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

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

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

Lecture 38

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

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

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

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

Lecture 39

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

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

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

4. Explain the difference between confusion and diffusion.

5. Is confusion or diffusion better for encryption?

Lecture 40

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

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

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

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

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

6. Is the Caesar Cipher algorithm strong?

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

CS361 Questions: Week 3

Lecture 41

1. Why are there 17576 possible decryptions for the “xyy” encoding on slide 3?

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

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

Lecture 42

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

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

3. Explain the key distribution problem.

Lecture 43

1. What is a downside to using encryption by transposition?

Lecture 44

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

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

3. If someonegets a hold ofKs, can heor she decrypt S’s encrypted messages? Why or why not?

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

Lecture 45

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

2. What is the significance of malleability?

3. What is the significance of homomorphic encryption?

Lecture 46

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

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

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

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

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

Lecture 47

1. What is a disadvantage in using ECB mode?

2. How can this flaw be fixed?

3. What are potential weaknesses of CBC?

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

Lecture 48

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

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

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

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

5. Comparetheefficiencyofasymmetricalgorithmsandsymmetricalgorithms.

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?

2. Explain the role of prime numbers in RSA.

3. Is RSA breakable?

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

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

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

7. How can someone intercepting $\{M\}_{K^{-1}_b}$ read the message?

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

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.

3. What is the difference between preimage resistance and second preimage resistance?

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

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

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

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

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

Lecture 51

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

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?

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

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

CS361 Questions: Week 3

Lecture 52

1. What would happen if g, p and $g_a$modp were known by an eavesdropper listening in on a Diffie-Hellman exchange?

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

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