Name: Ali Khan
EID: aak849
CS Login: alikhan
Email: alikhan@cs.utexas.edu

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?**
   It is impossible to have a better rate than C/h because C/h is the absolute perfect encoding of the entropy.

2. **How can increasing the redundancy of the coding scheme increase the reli- ability of transmitting a message over a noisy channel?**
   The message will get through after an arbitrary amount of tries.

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 diffi- cult?**
   Instances that other letters or symbols are more frequent than other letters and symbols

3. **Explain the difference between zero, first, second and third-order models.**
   Zero-order is the equal chance of any letter being picked. First-order involves the probability of a single letter being picked based off of the language. Second-order is the likelihood of two concurrent letters or symbols being chosen and third-order is the same as second-order except for it is three consecutive letters or symbols.

Lecture 36

1. **Why are prior probabilities sometimes impossible to compute?**
   Prior possibilities are completely different in all instances given different circumstances

2. **Why is the information content of a message relative to the state of knowl- edge of an observer?**
   The message relative to the knowledge of that observer can differ in entropy to the other observers.

3. **Explain the relationship between entropy and redundancy.**
   Entropy can be used to determine the redundancy in the encoding.

Lecture 37

1. **List your observations along with their relevance to cryptography about Captain Kidd's encrypted message.**
   *The encrypted message only uses the numbers 0-9 and the symbols *, +, :, ;, (,), +, and !.*

3. **Explain why a key may be optional for the processes of encryption or de- cryption.**
   There wouldn't be any use for a key if the decryption was just writing the document back words and not substituting letters for other symbols or letters.

4. **What effect does encrypting a file have on its information content?**
   Encrypting a text can render the text to be unreadable or not useful for any eavesdroppers accessing the file.

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

The eavesdropper can find similarities and patterns created by the encryption process to decrypt the file.

Lecture 38

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

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

3. **Why might a cryptanalyst want to recognize patterns in encrypted mes- sages?**
   Finding patterns and repetition of certain symbols can help them break an algorithm.

4. **How might properties of language be of use to a cryptanalyst?**
   Patterns within letters used in a language can be helpful for the analyst.

Lecture 39

1. **Explain why an encryption algorithm, while breakable, may not be feasible to break?**
   It may not be feasible to break because the only way to break it is through brute-force and that could take a lot of time.

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?**
   Because on average, most plaintext/ciphertext are cracked at around half way through the available key.

3. **Explain why substution and transposition are both important in ciphers.**
transposition They usually combined in most modern commercial symmetric ciphers for encryption and they have proved to be very useful.

3. **Explain the difference between confusion and diffusion.**
   Substitution tends to be good at confusion while transposition is good at diffusion.

4. **Is confusion or diffusion better for encryption?**
   Both are important because the combination of both maximizes the effects of the encryption.

Lecture 40

1. **What is the difference between monoalphabetic and polyalphabetic substi- tution?**
   A monoalphabetic cipher uses a 1-1 mapping of symbols, and a polyalphabetic substitution substitutes symbols based on where the symbol occurs in the plaintext.

2. **What is the key in a simple substitution cipher?**
   Number of rows

3. **Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?**
   Depending on how many symbols there are, there can be k possibilities for each symbol to have but cannot be repeated in that mapping.

4. **What is the key in the Caesar Cipher example?**
   Ciphertext designates the letter to be the letter two spaces ahead

5. **What is the size of the keyspace in the Caesar Cipher example?**
   26

6. **Is the Caesar Cipher algorithm strong?**
   No

7. **What is the corresponding decryption algorithm to the Vigenere ciphertextexample?**
   A polyalphabetic substitution

Lecture 41

1. Why are there 17576 possible decryptions for the "xyy" encoding on slide
3? *Because each space has a possibility of 26 letters*

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
Because y will have the same symbol and after the x is figured out there are 25 letters left to figure out the last two for y.

4. **Do you think a perfect cipher is possible? Why or why not?**
   A perfect cipher is not possible because there is always going to be a way to breach the computer security to crack the cipher

Lecture 42

1. **Explain why the one-time pad offers perfect encryption.**
   Take an arbitrary key plain text that is the same length as the plaintext and XOR'd it with the plaintext only once.

2. **Why is it important that the key in a one-time pad be random?**
   If you knew something about the key, working backwards and knowing the pattern could makeit possible to cut out half the keys based on the pattern.

3. **Explain the key distribution problem.**
   The sender and receiver have to have a secure channel to transfer the key to decrypt the cipher.

Lecture 43

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

Not strong because the symbols are rearranged but not substituted, and that leaves space for someone to have all the characters they need to decrypt the message.

Lecture 44

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

2. **Describe the difference between key distribution and key management.**
   Key distribution is who can have access to these keys and how to send them securely and key management is how to keep the abundance of keys secure from being accessed.

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

No they cannot because they do not have the private key.

3. **Are symmetric encryption systems or public key systems better?**
   Yes, because symmetric keys are easy to generate and are not as costly as public key systems.

Lecture 45

1. **Why do you suppose most modern symmetric encryption algorithms are block ciphers?**
   The block encryption makes it harder to decrypt based of the high diffusion and immunity to tampering and it is non-malleable.

2. **What is the significance of malleability?**
   Malleability allows an attacker to manipulate the ciphertext with predictable effects on plaintext.

3. **What is the significance of homomorphic encryption?**
   Homomorphic encryption is a form of encryption where a specific algebraic operation performed on the plaintext is equivalent to another algebraic operation performed on the ciphertext.

Lecture 46

1. **Which of the 4 steps in AES uses confusion and how is it done?**
   subBytes demonstrates confusion because they replace bytes by the value stored at that location.

2. **Which of the 4 steps in AES uses diffusion and how is it done?**
   shiftRows demonstrates diffusion by shifting the rows.

3. **Why does decryption in AES take longer than encryption?**
   It takes longer because the MixColumns step has to multiply by the inverse of the array and that is time consuming.

4. **Describe the use of blocks and rounds in AES.**
   AES allows keys of size 128-bits, 192-bits, and 256-bits, with 10, 12, 14 rounds, respectively.

5. **Why would one want to increase the total number of Rounds in AES?**
   More rounds would suggest the number of byte blocks to access and solve the decryption.

Lecture 47

1. **What is a disadvantage in using ECB mode?**
   Identical plaintext blocks contain the same encrypted blocks

2. **How can this flaw be fixed?**
   Use CBC

3. **What are potential weaknesses of CBC**
   An attacker can observe ciphertext over time to spot the first block that changed and there can be a content leak that allows the attacker to drive information about the two plaintext blocks.

4. **How is key stream generation different from standard block encryption modes**
5. *Bits appear random but they are actually not and it uses a one-time pad.*

Lecture 48

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

2. **Why are one-way functions critical to public key systems?**
   It is easily computed and near impossible to decrypt without additional information.

3. **How do public key systems largely solve the key distribution problem?**
   The public key can be seen by anyone but the only person who can decrypt is the person with the private key.

4. **Simplify the following according to RSA rules: $\{\{\{P\}_K{}^{-1}\}_K\}_K{}^{-1}$.**
   $\{P\}_K{}^{-1}$

5. **Compare the efficiency of asymmetric algorithms and symmetric algorithms.**
   Symmetric encryption plays the workhorse of most modern commercial encryption while asymmetric encryption has a few vital roles in the process.

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?**
   The keys are used in a symmetric fashion, which allows both keys to be used for decryption and encryption.

2. **Explain the role of prime numbers in RSA.**
   Prime numbers create a difficulty in factring the large numbers.

3. **Is RSA breakable?**
   Yes

4. **Why can no one intercepting $\{M\}_{Ka}$ read the message?**
   Because the person is not sure who is sending the message and the key could be different.

5. **Why can't A be sure $\{M\}_{Ka}$ came from B?**
   A cannot be sure because they are not using B's public key for authenticity.

6. **Why is A sure $\{M\}^{-1}$ originated with B?**
   A knows that B has access to B's keys and knows that they are the sender.

b

7. **How can someone intercepting $\{M\}^{-1}$ read the message?**
   They can save B's private key and find B's public key that is available and decrypt their message.

b

8. **How can B ensure authentication as well as confidentiality when sending a message to A?**
   A must have access to B's private key and send A the encrypted message using his public key.

Lecture 50

1. **Why is it necessary for a hash function to be easy to compute for any given data?**
   Because there is a fixed finite amount of hash values.

2. **What is the key difference between strong and weak collision resistance of a hash function.**
   A weak collision would be easy to find two messages that are equal, while strong collisions are based on the difficulty of finding two messages that are the same.

3. **What is the difference between preimage resistance and second preimage resistance?**
   A preimage is hard to find a value h based on the function f with message m. So it would be hard to find h = f(m). Second preimage is an example of a weak collision.

4. **What are the implications of the birthday attack on a 128 bit hash value?**
   $1.25*2^{64}$

5. **What are the implications of the birthday attack on a 160 bit hash value?**
   $1.25*2^{80}$

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

Document retrieval system containing legal records, it may be important to know that the copy retrieved is identical to that stored

7. **What attribute of cryptographic hash functions ensures that message M is bound to H (M), and therefore tamper-resistant?**
   It is tamper-resistant if computing the hash function of H(M) and then recomputing the file again. If H(M) is still the same after the recomputed, then the tamper-resistant conditions are met.

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

Lecture 51

1. **For key exchange, if S wants to send key K to R, can S send the following message: $\{\{K\}_{K_S^{-1}}\}_{K_R^{-1}}$? Why or why not?**
   No, because the confidentiality is breached using R's private key.

2. **In the third attempt at key exchange on slide 5, could S have done the en- cryptions in the other order? Why or why not?**
   No, because the confidentiality would be breached using S's private key at the end to R's public key.

3. **Is $\{\{\{K\}_{K_S^{-1}}\}_{K_R}\}_{K_S}$ equivalent to $\{\{K\}_{K_R^{-1}}\}_{K_R}$?**
   No, because R does not know S's private key, yet and cannot decrypt the final encryption.

4. **What are the requirements of key exchange and why?**
   Key exchange must ensure confidentiality and authentication.

Lecture 52

1. **What would happen if g, p and $g^a \bmod p$ were known by an eavesdropper listening in on a Diffie-Hellman exchange?**
   If they do not know b, they cannot find out anything based on the information they have.

2. **What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?**
   Nothing

3. **What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?**
   the eavesdropper can find the value and crack the cipher.