NAME: Ali Pasha
UTEID: aap2493
CSACCOUNT: alipasha
EMAIL: alipasha@utexas.edu

CS361 Questions: Week 3

The questionsmarked 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?
   Because if that were possible, then you would have found a coding scheme better than entropy, which is impossible.

2. How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?
   Because the fundamental theorem of a noisy channel states that as long as a channel can physically handle the message traffic, then if you keep trying to push the message through, it will eventually get to the receiver.

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?
   Log(10) = approximately 3.32 (where the log is base 2).

2. What are reasons why computing the entropy of a natural language is difficult?
   Because the symbols are not independent of each other, and are instead highly dependent on many factors.

3. Explain the difference between zero, first, second and third-order models.
   Zero-order assumes independence and equally likely, first-order assumes independence but not equally likely, third-order drops both assumptions, and the increasing orders add additional dependencies.

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?
   Because it is impossible to know them.

2. Why is the information content of a message relative to the state of knowledge of an observer?
Because the information content depends on how much the observer already know. If the observer knows everything in the message, then the information content is zero.

3. Explain the relationship between entropy and redundancy.
Entropy is the measure of redundancy. The better the entropy (smaller entropy value), the less redundancy there is.

Lecture 37

1. List your observations along with their relevance to cryptography about Captain Kidd's encrypted message.
This is wacko, not dot.

2. Explain why a key may be optional for the processes of encryption or decryption.
If the encryption process itself is sufficient in producing cipher text that cannot be broken, then a key may not be necessary.

3. What effect does encrypting a file have on its information content?
Hide the information content without destroying it.

4. How can redundancy in the source give clues to the decoding process?
Redundancy can give clues by showing possible patterns.

Lecture 38

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

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

3. Why might a cryptanalyst want to recognize patterns in encrypted messages?
To do such things as traffic analysis.

4. How might properties of language be of use to a cryptanalyst?
It might help detect patterns, such as frequency of symbols in English.

Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?
Because it might take an unreasonable amount of time to break.

2. Why, given a small number of plaintext/ciphertext pairs encrypted under key K, can K be recovered by exhaustive search in an expected time on the order of 2^{n-1} operations?
Because on average, that's how long it takes.

3. Explain why substitution and transposition are both important in ciphers.
Because when used in combination they are very powerful.

4. Explain the difference between confusion and diffusion.
Confusion transforms the text so that the interceptor cannot readily extract it, while diffusion spreads the information widely over the ciphertext.

5. Is confusion or diffusion better for encryption?
They each serve a different goal.

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substitution?
Monoalphabetic is when each symbol of the text is uniformly exchanged for another, while polyalphabetic uses different substitutions depending where in the text the symbol occurs.

2. What is the key in a simple substitution cipher?
However the 1-1 mapping is specified.

3. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?
Because for a set of k elements, there are k! mappings of the set onto itself. In simple substitution, there are k! ways to rearrange the 1-1 mappings.

4. What is the key in the Caesar Cipher example?
How many positions you shift.

5. What is the size of the keyspace in the Caesar Cipher example?
25 or 26 depending on how you look at it.

6. Is the Caesar Cipher algorithm strong?
Probably not.

7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?
Doing the inverse of the encryption algorithm.

Lecture 41

1. Why are there 17576 possible decryptions for the "xyy" encoding on slide 3?
Assuming it's not a simple substitution, there are 26 letters and 3 letters in the string "xyy" with different displacements, so 26^3 = 17576.

2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
   Because it is a simple substitution, so now there's just one substation for both "y" in "xyy" and the substitutions are done without replacement.

3. Do you think a perfect cipher is possible? Why or why not?
   Not according to the definition.

Lecture 42

1. Explain why the one-time pad offers perfect encryption.
   Because every possible plaintext could be the pre-image of that ciphertext under a plausible key. Hence, no reduction of the search space is possible.

2. Why is it important that the key in a one-time pad be random?
   Having any info about the key would allow one to work backwards and eliminate parts of the key space.

3. Explain the key distribution problem.
   Since the key is as long as the plaintext, how can the key be securely transmitted? If through a secure channel, then why not just send the plaintext through that channel? And if not a secure channel, then how can they securely distribute the key?

Lecture 43

1. What is a downside to using encryption by transposition?
   It only serves in diffusing, and so, the frequencies of the letters are preserved.

Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?
   It is symmetric since the key is the same.

2. Describe the difference between key distribution and key management.
   Key distribution is concerned with how to convey keys to those that need them to establish secure communication, while key management is concerned with how to preserve the safety of a large number of keys and make them available as needed.

3. If someone gets a hold of Ks, can he or she decrypt S's encrypted messages? Why or why not?
   No, because Ks is public, and the only way to decrypt S's encrypted message is to use K's private key, Ks-1.

4. Are symmetric encryption systems or public key systems better?
   Symmetric encryptions are better since they are O(n^2) while public encryptions are O(n)

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
   Because of immunity to tampering and high diffusion.

2. What is the significance of malleability?
   Malleability can bring about meaningful changes in the plaintext without anyone knowing that the ciphertext was tampered with.

3. What is the significance of homomorphic encryption?
   Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked with as if it were still in its original form.

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?
   In the second step by doing a lot of multiplication of matrices.

2. Which of the 4 steps in AES uses diffusion and how is it done?
   In the third step by doing a lot of abracadabra.

3. Why does decryption in AES take longer than encryption?
   It's because you have to multiply by an inverse matrix.

4. Describe the use of blocks and rounds in AES.
   You take a block, go round and round, mangling it further and further, until your done.

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

Lecture 47

1. What is a disadvantage in using ECB mode?
   Identical blocks in the plaintext yield identical blocks in the ciphertext.

2. How can this flaw be fixed?
   By using cipher block chaining.

3. What are potential weaknesses of CBC?
   An attacker can observe changes, and content leak.

4. How is key stream generation different from standard block encryption modes?
   In key stream generation the cipher is used more as a pseudorandom number generator.

Lecture 48

1. For public key systems, what must be kept secret in order to ensure secrecy?
    The key that hold all secrets must be kept secret, assuming it exists.

2. Why are one-way functions critical to public key systems?
    They are the basis of any public key system.

3. How do public key systems largely solve the key distribution problem?
    Because you don't have to worry about sending keys securely.

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.
    Asymmetric are much less efficient than symmetric algorthms.

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?
    It would, but everything would become goobly gobbly.

2. Explain the role of prime numbers in RSA.
    Prime numbers are impossible to figure out using a formula.

3. Is RSA breakable?
    No.

4. Why can no one intercepting $\{M\}_{K_a}$ read the message?
    Because that's just life.

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

6. Why is A sure $\{M\}_{K^{-1}b}$ originated with B?
    Because, although B may have some issues, B is a pretty good person in general

7. How can someone intercepting $\{M\}_{K^{-1}b}$ read the message?
    By asking someone who knows how to read it.

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

Lecture 50

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

2. What is the key difference between strong and weak collision resistance of a hash function.
    Asdf asdf wekj fl/.

3. What is the difference between preimage resistance and second preimage resistance?
    The first is if any m is hard to find, the second is for m2 != m1.

4. What are the implications of the birthday attack on a 128 bit hash value?
    Birthdays should not be had with 128 bit hash values.

5. What are the implications of the birthday attack on a 160 bit hash value?
    Birthdays with 160 bits may be ok, but don't get carried away.

6. Why aren't cryptographic hash functions used for confidentiality?
    Because they are used for integrity.

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

8. Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?
    RSA is wak, so B just walks over to A.

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following message: $\{\{K\}_{K_{S^{-1}}}\}_{K^{-1}_R}$? Why or why not?
    What kind of question is this (no question mark here).

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?
    Yes. No.

3. Is $\{\{\{K\}_{K_{S^{-1}}}\}_{K_R}\}_{K_S}$ equivalent to $\{\{K\}_{K^{-1}_S}\}_{K_R}$?
    Yes.

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

It should be done in a manner unknown to all except the exchanging parties, so preferably under the doormat.

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?

The eavesdropper would be hurt because g and p always talk mess about gamodp.

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

The eavesdropper would beat up a.

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

As mentioned before, b is a pretty nice person, so everyone would just let it go.