Freda Anderson fa3365
Freda.Ander@gmail.com

CS361 Questions: Week 3

Lecture 34

1. Why is it impossible to transmit a signal over a channel at an average rate greater than C/h?
   a. Because you can't transmit more data across the channel (the "pipe" is full).
2. How can increasing the redundancy of the coding scheme increase the reliability of transmitting a message over a noisy channel?
   a. There is more redundant data to find if you missed something

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?
   a. H = -(log10)
2. What are reasons why computing the entropy of a natural language is difficult?
   a. It is difficult to model – some symbols appear often, some appear in groups of two or three with much more frequencies than others.
3. Explain the difference between zero, first, second and third-order models.
   a. Zero Order Model – we assume that all characters are equally likely
   b. First Order Model – we assume that some symbols are more likely
   c. Second Order Model – we assume some bi-letter strings are more likely
   d. Third Order Model – we assume some 3 letter strings are more likely

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?
   a. Some strings are random and entropy is relative to a particular observer
2. Why is the information content of a message relative to the state of knowledge of an observer?
   a. Someone might know the answer and another person might not. It depends on their uncertainty
3. Explain the relationship between entropy and redundancy.
   a. Entropy can be used to calculate redundancy. If the message and encoding are equal, then there is no redundancy.

Lecture 37

1. List your observations along with their relevance to cryptography about Captain Kidd's encrypted message.
   a. The more frequent a symbol is, the more likely it's a common English character.
2. Explain why a key may be optional for the processes of encryption or decryption.
   a. If you have a key, you can look up or compute a symbol's meaning.

3. What effect does encrypting a file have on its information content?
    a. It obscures the meaning of a text
4. How can redundancy in the source give clues to the decoding process?
    a. The more frequent the letter the more likely it is a common English letter like e, t, r and or s.

Lecture 38

1. Rewrite the following in its simplest form: $D(E(D(E(P))))$.
    a. P
2. Rewrite the following in its simplest form: $D(E(E(P,K_E),K_E),K_D)$.
    a. $E(P,K_E)$
3. Why might a cryptanalyst want to recognize patterns in encrypted messages?
    a. Break an encryption and/or study its weaknesses
4. How might properties of language be of use to a cryptanalyst?
    a. Looks for redundancy in both language and cipher

Lecture 39

1. Explain why an encryption algorithm, while breakable, may not be feasible to break?
    a. You can always brute force an encryption algorithm to break it, however, some encryptions can take thousands (or more) of years to try each and every possibility.
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?
    a. Because there are only a certain number of ways an n bit string can appear as.
3. Explain why substitution and transposition are both important in ciphers.
    a. Substitution tends to be good at confusion; transposition tends to be good at diffusion
4. Explain the difference between confusion and diffusion.
    a. Confusion makes an interceptor unable to readily extract information while diffusion spreads information around.
5. Is confusion or diffusion better for encryption?
    a. You need both.

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substitution?
    a. Monoalphabetic substitution is done uniformly. Polyalphabetic is done where in the plaintext the symbol occurs.
2. What is the key in a simple substitution cipher?
    a. The key is a one to one mapping. For instance replace every a with b, every b with c and so one.
3. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?
    a. Because you are mapping one language with k letters onto another. There are k! ways of doing this.
4. What is the key in the Caesar Cipher example?

    a. The key is a one to one mapping where every letters is just n away from its mapping.
5. What is the size of the keyspace in the Caesar Cipher example?
    a. Keyspace is k-1.
6. Is the Caesar Cipher algorithm strong?
    a. No the algorithm is not strong.
7. What is the corresponding decryption algorithm to the Vigenere ciphertext example?
    a. You have to have the original key and use the look up table.

Lecture 41

1. Why are there 17576 possible decryptions for the "xyy" encoding on slide 3?
    a. Because there are 26 letters in the alphabet and three places. XY can be the same symbols or YY can be different symbols if they used a polyalphabetic cipher.
2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
    a. Because now we know that Y and Y are the same letters.
3. Do you think a perfect cipher is possible? Why or why not?
    a. Theoretically, but I don't think so.

Lecture 42

1. Explain why the one-time pad offers perfect encryption.
    a. There is no reduction of the search space.
2. Why is it important that the key in a one-time pad be random?
    a. If its not, then there could be an algorithm to get the key.
3. Explain the key distribution problem.
    a. An unwanted third party could get the key by someone who knows the algorithm and the seed.

Lecture 43

1. What is a downside to using encryption by transposition?
    a. It preserves letter frequencies.

Lecture 44

1. Is a one-time pad a symmetric or asymmetric algorithm?
    a. Symmetric
2. Describe the difference between key distribution and key management.
    a. Key Distribution is about getting keys to people securely. Key management is about preserving key safety and making them available.
3. If someone gets a hold of Ks, can he or she decrypt S's encrypted messages? Why or why not?
    a. Not if its asymmetric. In a public key encryption, different keys are used for encryption and decryption, having one of K's keys is not enough.
4. Are symmetric encryption systems or public key systems better?
    a. Depends. Symmetric keys are simple to generate and have no special properties, while public keys have a special structure.

Lecture 45

1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
    a. Block ciphers are immune to tampering and can have high diffusion.
2. What is the significance of malleability?
    a. You can't transform ciphertext once it has be encrypted, you will get different data.
3. What is the significance of homomorphic encryption?
    a. They are malleable and preserve operations.

Lecture 46

1. Which of the 4 steps in AES uses confusion and how is it done?
    a. subBytes – use a lookup table
    b. shiftRows – shift rows of the block
2. Which of the 4 steps in AES uses diffusion and how is it done?
    a. mixColumns
    b. addRoundKey – XOR the state with a 128 bit round key
3. Why does decryption in AES take longer than encryption?
    a. You use a different fix matrix in the mixColumns step.
4. Describe the use of blocks and rounds in AES.
    a. A block is a small matrix of data that gets transformed and substituted in rounds during the AES decrypt/encrypt.
5. Why would one want to increase the total number of Rounds in AES?
    a. You have to decrypt with a certain number of rounds, by changing it

Lecture 47

1. What is a disadvantage in using ECB mode?
    a. Leaves too much regularity in the ciphertext.
2. How can this flaw be fixed?
    a. You can chain some blocks together.
3. What are potential weaknesses of CBC?
    a. An attacker can observe changes over time and will be able to spot the first block that changed.
    b. If an attacker can spot two identical blocks, he can derive information about two plain text blocks.
4. How is key stream generation different from standard block encryption modes?
    a. A key stream generation can be used as in one-time pad.

Lecture 48

1. For public key systems, what must be kept secret in order to ensure secrecy?
    a. A person must have a secret key to decrypt.
2. Why are one-way functions critical to public key systems?
    a. It is easy to compute, but difficult to invert without additional information.
3. How do public key systems largely solve the key distribution problem?

   a. They use one way functions?
4. Simplify the following according to RSA rules: $\{\{\{P\}_{K-1}\}_K\}_{K-1}$.
   a. $\{P\}_{K-1}$
5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.
   a. Asymmetric algorithms are generally much less efficient than symmetric algorithms.

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?
   a. Yes, you just need to keep one of the keys private.
2. Explain the role of prime numbers in RSA.
   a. Both parties pick a number and send their number to each other. Using the equation $\{\{P\}_d\}_e = P = \{\{P\}_e\}_d$ they get the same number.
3. Is RSA breakable?
   a. Theoretically very secure because it uses NP Complete problems that can be checked in polynomial time.
4. Why can no one intercepting $\{M\}_{Ka}$ read the message?
   a. They will need A's private key.
5. Why can't A be sure $\{M\}_{Ka}$ came from B?
   a. Because there is no identification tagged with the message.
6. Why is A sure $\{M\}_{K-1b}$ originated with B?
   a. Because A needs to use B's public key – which means it was encrypted using B's private key.
7. How can someone intercepting $\{M\}_{K-1b}$ read the message?
   a. Because B's key is public.
8. How can B ensure authentication as well as confidentiality when sending a message to A?
   a. $\{\{M\}_{kb-1}\}_{ka}$

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.
   a. A strong collision resistant is hard to find two messages m1 and m2 such that f(m1) = f(m2).
3. What is the difference between preimage resistance and second preimage resistance?
   a. Preimage resistance is about inverting the hash, second preimage resistance is about collisions caused by two messages mapping to the same hash.
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?
   a. Hashing makes alterations apparent. Anyone can decrypt if they have the algorithm.

7. What attribute of cryptographic hash functions ensures that message M is bound to H(M), and therefore tamper-resistant?
    a. Anytime the file is used, rehash it and compare it to the original.
8. Using RSA and a cryptographic hash function, how can B securely send a message to A and guarantee both confidentiality and integrity?
    a. RSA ensures confidentiality and cryptographic hash ensures 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?
    a. No, S shouldn't have R's key and a third party can decrypt K-1R using R's public key.
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?
    a. No, because a third party could decrypt it using S's public key.
3. Is $\{\{\{K\}_{KS-1}\}_{KR}\}_{KS}$ equivalent to $\{\{K\}_{K-1S}\}_{KR}$?
    a. Yes
4. What are the requirements of key exchange and why?
    a. Confidentiality and authentication – you don't want to share private information with the wrong person.

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?
    a. The eavesdropper still doesn't have the key.
2. What would happen if a were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
    a. The eavesdropper could get the key.
3. What would happen if b were discovered by an eavesdropper listening in on a Diffie-Hellman exchange?
    a. They eavesdropper can get the key.