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?

Because you cannot do better than entropy.

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

Because eventually the message will get across if you increase redundancy.

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 = -(10 * 1/10 log 1/10) = - (log.1)

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

Calculating the true entropy of a language requires higher and higher order models.

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

Zero order models state all symbols equally likely. First order calculates likelihood of a symbol. Second order calculates likelihood of a symbol after a certain symbol. And so on...

Lecture 36

1. Why are prior probabilities sometimes impossible to compute?

You do not have the necessary information to determine the likelihood of an outcome.

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

If an observer knows more than another, they can more accurately guess the likelihood of the message.

3. Explain the relationship between entropy and redundancy.

Entropy is used to determine the amount of redundancy.

Lecture 37

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

2. Explain why a key may be optional for the processes of encryption or de-cryption.

If no one else knows the encryption algorithm, then there is no need for an additional layer of security.

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

Transforms the information content into something (ideally) indecipherable to a regular observer.

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

Repeated sequences can give clues. For instance, if the text is a basic encrypted english document and a repeated sequence happens N% of the time, then you can look for words that happen around the same likelihood. From there you can potentially figure out the letters. You can go from there and build a bigger and bigger cipher that helps decode the message.

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 mes-sages?

Patterns can be used to build a cipher that decodes the message.

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

Likelihood of words, letters, grammatical structures all can assist in building a cipher.

Lecture 39

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

It requires brute forcing every possible combination.

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 2n−1 operations?

You can progress through entire keyspace finding keys that match a plaintext/ciphertext pair.

Keys that work can be checked against other pairs. If key works for all pairs, then it is correct key.

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

Substitution increases confusion. Transposition increases diffusion.

4. Explain the difference between confusion and diffusion.

Confusion: transformations increasing difficulty to extract information, Diffusion: transformations spreading plaintext throughout the ciphertext.

5. Is confusion or diffusion better for encryption?

They're both equally important in encrypting a message and are both used in modern encryption.

Lecture 40

1. What is the difference between monoalphabetic and polyalphabetic substi-

tution?

Monoalphabetic is a 1-1 mapping for symbol substitution. Polyalphabetic substitutes symbols contextually within the plaintext.

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

The mapping of one symbol to the other symbol.

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

substitution?

Because there are only a limited number of 1-1 mappings possible.

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

the key is 'CDEFGHIJKLMNOPQRSTUVWXYZAB'.

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

26!

6. Is the Caesar Cipher algorithm strong?

No. It can be deciphered contextually too.

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

example?

Go to corresponding row for letter in key, find column which ciphertext letter is in. The column is the plaintext letter.

Lecture 41

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

“xyy” can represent no more than 3 characters otherwise information is lost. Therefore there are up to 26^3 possibilities.

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

You now only have 2 letters that are simply substituted. 1 has 26 possibilities and the other has 25 because the 26th possibility is taken up by the other letter.

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

Yes. Sending only a single message with a certain key with enough redundancy is impossible to crack. One time PADs are examples of perfect ciphers.

Lecture 42

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

A properly executed one-time pad has the characteristic that if a ciphertext is intercepted there is no possible reduction in keyspace.

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

If the keys weren’t random then that adds a point of vulnerability. Systematic generation can be broken.

3. Explain the key distribution problem.

A key must be given to the two communicators beforehand and can only be used once to be properly executed.

Lecture 43

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

Letter frequencies, etc are still retained.

Lecture 44

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

Symmetric

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

distribution - conveying key to those that need them for secure comm. management - safely storing keys and make them available when needed.

3. If someone gets a hold of Ks, can he or she decrypt S’s encrypted messages?

Why or why not?

No, Ks is the public key. A message encrypted with Ks can only be decrypted with the private key (K-1s).

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

That distinction is purely contextual. public keys are expensive to generate, symmetric keys are hard to disseminate.

Lecture 45

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

block ciphers?

Block ciphers give the ability to encrypt chunks of symbols rather than individual symbols.

2. What is the significance of malleability?

Malleability describes the ability for an attacker to alter plaintext contents systematically by altering the ciphertext. This is an integrity issue.

3. What is the significance of homomorphic encryption?

Certain transformations can be performed on ciphertexts with results mirroring the results of performing said transformations on the plaintext itself. Information about the plaintext can be extracted without decrypting.

Lecture 46

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

subbytes. Substitutes bytes increasing confusion.

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

mixColumns uses transposition to introduce diffusion into the encryption

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

the inversion of mixcolumns takes longer to do matrix multiplication with. decryption uses the inversion of mixcolumns.

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

an n-bit block is encrypted by going through k rounds of an encryption process.

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

As you increase in rounds, you increase the confusion and diffusion. Thus, making cracking more difficult.

Lecture 47

1. What is a disadvantage in using ECB mode?

Systematic patterns can be found from identical sections of plaintext being encoded similarly

2. How can this flaw be fixed?

Adding some form of diffusion to the encryption algorithm, and possibly multiple rounds worth.

3. What are potential weaknesses of CBC?

If an attacker can find two identical ciphertext blocks, he can learn something about the algorithm/plaintext blocks.

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

It uses the cipher to generate a random number that can be used as a one-time pad.

Lecture 48

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

the private key.

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

It is part of the fundamental concept of public key systems. more than one-way functions would require all communicators to have the key, causing a higher security vulnerability.

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

They publish their public keys relatively loosely as public keys can only encrypt.

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 algorithms are order of magnitudes more expensive to compute 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?

Yes {{P}d}e = P = {{P}e}d.

2. Explain the role of prime numbers in RSA.

Products of two prime number are incredibly hard to factor compared to their ease to compute.

3. Is RSA breakable?

Yes, by brute force.

4. Why can no one intercepting {M}Ka read the message?

A’s private key is required to decrypt the message.

5. Why can’t A be sure {M}Ka came from B?

A’s public key is public information and isn’t signed like in other public key systems.

6. Why is A sure {M}K−1b originated with B?

Only B has his own private key for encryption.

7. How can someone intercepting {M}K−1b read the message?

B’s public key.

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

Encrypt with B's private key and A's public key.

Lecture 50

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

The data can be very large.

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

Weak collision resistance - hard to find another match to a previously given random string's hash.
Strong collision resistance - hard to find another match to any given string.

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

Preimage resistance describes diifculty in finding an m such that h = f(m). Second preimage resistance is synonymous with weak collision resistance.

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

It would take 2.306e19 evaluations to find a pair x,y with matching hash values.

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

1.511e24 evaluations

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

It may be more important to know if a transmission wasn't corrupted.

7. What attribute of cryptographic hash functions ensures that message M is

bound to H(M), and therefore tamper-resistant?

It is uncommon for other M's to compute to the same hash value. Therefore, if the calculated H is different than previously then M has most likely changed.

8. Using RSA and a cryptographic hash function, how can B securely send a

message to A and guarantee both confidentiality and integrity?

public key systems like RSA are used for confidentiality, whereas cryptographic hash functions are used for integrity.

Lecture 51

1. For key exchange, if S wants to send key K to R, can S send the following

message: $\{\{K\}KS-1\}KR-1$? Why or why not?

No that would require R's private 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?

It would remove authentication but it could still work possibly.

3. Is $\{\{\{K\}KS-1\}KR\}KS$ equivalent to $\{\{K\}K-1S\}KR$?

Nope.

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

encrypting with private key ensures authenticity, encrypting with public key ensures confidentiality. Ideally we want both.

Lecture 52

1. What would happen if g, p and gamodp were known by an eavesdropper

listening in on a Diffie-Hellman exchange?

a and b are still unknown so there is no harm done.

2. What would happen if a were discovered by an eavesdropper listening in on

a Diffle-Hellman exchange?

The secret key would be compromised.

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

Same as #2.