**Lecture 34**

1. Why is it impossible to transmit a signal over a channel at an average rate greater than C/h?

Yes it is impossible, because the pipe which data is being sent through has a max bandwidth of C/h

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

It makes the receiver surer of the message he is receiving. You could transmit the same message 1000 times just to make sure the message was received properly

**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 1/10) = 3 point something = would require 4 bits

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

There are too many different endings/redundancies to calculate it accurately

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

The second order model shows the likely hood of a character following a particular character. Third order model shows common 3 letter combinations (because the letters are usually paired with eachother)

**Lecture 36**

1. Why are prior probabilities sometimes impossible to compute?

 Because you don’t know the knowledge level of the receiver/observer.

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

Because if the observer thinks all 5 outcomes are equally likely then the entropy would be log(1/5), but if the observer knows that some outcomes are more likely than others then the entropy would be less than log(1/5)

1. Explain the relationship between entropy and redundancy.

The lower the redundancy, the lower the entropy.

**Lecture 37**

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

All of the characters are from the same row on the keyboard (numbers and math characters)

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

A key can show you the values that need to be substituted.

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

It distorts the text, but shouldn’t have any affect on the information contained (if the key is used)

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

Knowing redundancies in the text, the attacker could formulate the key by knowing the frequencies that letters are repeated.

**Lecture 38**

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

P(P)

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

P(P(C))

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

If the cryptanalyst knows a piece of the translation, it could make it easier to figure out the translation or key

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

Redundancies can reveal character occurrences. Message beginnings such as “hello” or common word endings such as “-tion” and “ing” could lead to encryption revelations

**Lecture 39**

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

It is breakable because their has to be a possible key, but most times there are too many possible combinations to go through in order to test all of them (would take too long).

1. 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 2n−1 operations?

Because assuming using a linear search method, it takes on average half of the possibilities to find the encryption (which is 2^n-1)

1. Explain why substitution and transposition are both important in ciphers.

They both create confusion and diffusion (make problems regaining the original method)

1. Explain the difference between confusion and diffusion.
   1. Confusion causes trouble for the attacker to extract the original symbol, diffusion spreads information around across the message.
2. Is confusion or diffusion better for encryption?

A combination of both methods is needed for a strong encryption.

**Lecture 40**

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

Monoalphabetic shifts each letter circulary a certain amount of letters, polyalphabetic uses a key to index into a table of characters of cesear ciphers.

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

A 1 to 1 mapping of one character to any other chosen one.

1. Why are there k! mappings from plaintext to ciphertext alphabets in simple substitution?
2. What is the key in the Caesar Cipher example?

The amount of characters you shift is the key

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

26 different keys since that is the total number of different variations you can shift by.

1. Is the Caesar Cipher algorithm strong?

No, it can be easily decrypted

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

A table of Caesar cipher shifts (Vigenere tableau), you can also use statistics to find more popular characters aka it isn’t completely random.

**Lecture 41**

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

26\*26\*26

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

Since the first two letters are different, and the last two letters are the same, there are only 26\*26 possible decryptions

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

Yes, because an encryption can be dynamic/random.

**Lecture 42**

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

XOR the key and the plaintext

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

If you knew that the key had an even number of 1 bits, you could eliminate half of the plain text by working backwards.

3. Explain the key distribution problem.

How do you get the key to the other side of the channel? You would need a secure channel, but that is what the key is supposed to be used for

**Lecture 43**

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

It only moves the characters around in the text, not changing any of the text (letter frequencies are preserved).

**Lecture 44**

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

Symmetric.

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

Distribution is about getting a key to the other party that needs it, while management is preserving the safety of the keys and only providing the ones that are needed

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

No, even if they can encrypt a message there is a different key to encrypt the message

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

Both have benefits, but symmetric encryptions are stronger in terms of number of bits needed for the key.

**Lecture 45**

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

High diffusion (each character doesn’t affect the next), and immunity to tampering

1. What is the significance of malleability?

Malleability are generally bad in ciphers. It allows you to determine if the meaning of the message has changed

1. What is the significance of homomorphic encryption?

It is significant because every block could affect the next block if it is messed up. Homomorphic encryption enables the message to be encrypted/decrypted the same way.

**Lecture 46**

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

SubBytes

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

shiftRows and mixColumns

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

Because when you multiply by the inverse of the array, the values are larger than the original 1, 2, and 3 scales

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

The block size allows 128+ bits to be encrypted/decrypted at once, each block undergoes the four rounds of the AES process to be encrypted/decrypted

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

To increase the difficulty of decoding the cipher or to encode larger block sizes.

**Lecture 47**

1. What is a disadvantage in using ECB mode?

If there are identical lines in the plain text, it would output identical lines in the cipher text

1. How can this flaw be fixed?

This can be fixed by randomizing the plain text blocks by cipher chaining. You XOR with the previous string

1. What are potential weaknesses of CBC?

Since the first block encrypted isn’t xor’ed with anything it could lead to weaknesses on the other lines.

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

It is a pseudorandom number generator 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 decryption key.

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

They allow everyone to create encrypted files, but only people with the decryption key can actually interpret the message

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

It sends the encryption key to everyone, we don’t really care about secrecy of that key. We only need to keep the decryption key secret

4. Simplify the following according to RSArules:{{{P}K−1}K}K−1.

P

5. Compare the efficiency of asymmetric algorithms and symmetric algorithms.

Symmetric algorithms are 10,000x faster and more effiecint than asymmetric systems, because they require factoring of large prime numbers and modular arithmetic instead of bitwise operations

**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 algorithm would still work because the method can be inversed, however it wouldn’t be secure anymore.

1. Explain the role of prime numbers in RSA.

In using the knapsack problem, it is difficult to find the exact pattern of factors to achieve a prime number in real time, where as if you know the factors before hand you can check the calculation very quickly.

1. Is RSA breakable?

No. It can be used for authenticity or privacy, but not both at once.

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

Because they don’t have the {M}k^-1 key

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

Because it is a public key, and anyone could have encrypted the message

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

Because B is the only person with that key (private key) so it had to come from him.

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

By using the public key, {M}Ka

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

He could use 2 sets of keys, one for authentication, and another for confidentiality

**Lecture 50**

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

Because you need to map the values to their corresponding hash value quickly.

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

Weak collision assumes that you have one value and its hash, it is difficult to find another value that maps to the same hash. Strong collision makes it difficult for any 2 values to map to the same hash

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

Preimage resistant is that given the hash, it is hard to find a value that matches that hash, while second preimage resistance is the same as weak collision as descried above in question 2.

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

 On average, you will have to look at 1.25\*(2^64) values before you find a collision

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

On average, you will have to look at 1.25\*(2^80) values before you find a collision

1. Why aren’t cryptographic hash functions used for confidentiality?

We want to see if the value you sent is the same value that the other party received, which isn’t guaranteed using a hash function.

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

Preimage and strong collision resistance

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

Send the message using RSA key and then use the hash function to verify that the integrity of the message is the same (by checking that it still maps to the same hash value)

**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−1? Why or why not?

No, the private key needs to be on the outside of the function to provide confidentiality.

1. In the third attempt at key exchange on slide 5, could S have done the encryptions in the other order? Why or why not?

No, the authentication must be checked first, and then check that the person has the correct authentication. If it was done in the other order, the authorization could still be seen from the shared public key

1. Is {{{K}KS−1}KR}KS equivalent to {{K}K−1}KR?

 no. You don’t need Ks on the outside of the formula

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

Confidentiality (make sure outsiders cannot read the information coming in) and authorization (make sure you know who the information is coming from)

**Lecture 52**

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

Nothing, without knowing A or B, the other values are worthless and don’t help decoding the messages being exchanged

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

Knowing A, the eavesdropper could decode the messages sent by alice

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

Knowing B, the eavesdropper could decode the messages sent by Bob