UTEID: dpk326;
FIRSTNAME: David;
LASTNAME: Ko;
CSACCOUNT: davidko;
EMAIL: davidpeterko@gmail.com;

CS361 Questions: Week 3
These questions relate to Modules 8, 9, 10 and 11. Type your answers and submit
them on Canvas by 5pm on Thursday, June 25.

Lecture 34
1. Why is it impossible to transmit a signal over a channel at an average rate
greater than C/h?
Because you cant send more bits than it can physically handle
2. How can increasing the redundancy of the coding scheme increase the reliability
of transmitting a message over a noisy channel?
lost for package due to loss of bits

Lecture 35
1. If we want to transmit a sequence of the digits 0–9. According to the zeroorder
model, what is the entropy of the language?
-log(1/10)
2. What are reasons why computing the entropy of a natural language is diffi-
cult?
because even if you scramble the letters and have a high pass rate, you can still be missing letters
3. Explain the difference between zero, first, second and third-order models.
zero: naive
first: accounts for probability of usage
second: accounts for pairs of letters
third: accounts sequences of consequent letteers

Lecture 36
1. Why are prior probabilities sometimes impossible to compute?
you dont know all the info
2. Why is the information content of a message relative to the state of knowledge
of an observer?
from the lecture video: the academy awards
3. Explain the relationship between entropy and redundancy.
if the encoding and entropy match, there is no redundancy

Lecture 37
1. List your observations along with their relevance to cryptography about
Captain Kidd’s encrypted message.
	the numbers could be locations, end lines, and we dont know what language it is in
2. Explain why a key may be optional for the processes of encryption or decryption.
	having a pubylic or private key makes it harder for the attacker to decrypt
3. What effect does encrypting a file have on its information content?
	it creates a ciphertext that other people cant read
4. How can redundancy in the source give clues to the decoding process?
	all encrypted data can have redundancy

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, KE), KE), KD).
	E(P, KE)
3. Why might a cryptanalyst want to recognize patterns in encrypted messages?
	gives clues on the redundancy in the ciphertext
4. How might properties of language be of use to a cryptanalyst?
	redundancies can be present

Lecture 39
1. Explain why an encryption algorithm, while breakable, may not be feasible
to break?
	You have to runn all possible combinations within the given 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 2n−1 operations?
		# of possible keys
3. Explain why substution and transposition are both important in ciphers.
	substituion -> confusion and transposition -> diffusion
4. Explain the difference between confusion and diffusion.
	Confusion is replacing a simple piece of data, causign trouble to obtain the raw data where diffusion moves it away from its location
5. Is confusion or diffusion better for encryption?
	both are important

Lecture 40
1. What is the difference between monoalphabetic and polyalphabetic substitution?
mono is done uniformly, where poly is done based on symbols and locations
2. What is the key in a simple substitution cipher?
the letter itself
3. Why are there k! mappings from plaintext to ciphertext alphabets in simple
substitution?
it is a 1 to 1 mapping
4. What is the key in the Caesar Cipher example?
the ltter itself
5. What is the size of the keyspace in the Caesar Cipher example?
k!
6. Is the Caesar Cipher algorithm strong?
no because it is a 1 to 1 mapping
7. What is the corresponding decryption algorithm to the Vigenere ciphertext
example?
finding the key and the encryption text and finding which one they are

Lecture 41
1. Why are there 17576 possible decryptions for the “xyy” encoding on slide
3?
each letter x or y could map to a different letter
2. Why is the search space for question 2 on slide 3 reduced by a factor of 27?
y and only map to itself so it reduces by a factor of 27
3. Do you think a perfect cipher is possible? Why or why not?
yes the combinations are endless

Lecture 42
1. Explain why the one-time pad offers perfect encryption.
keys are random, it is impossible to detect even if you have the plaint text
2. Why is it important that the key in a one-time pad be random?
oehterwise the attacker can distinguish between responses from the challenger
3. Explain the key distribution problem.
the key distribution must be completely random (non deterministic)

Lecture 43
1. What is a downside to using encryption by transposition?

brute force

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 is how to convey keys and estabish a secure connection whereas management is given all the key and has to find a way to kepe them safe but available
3. If someone gets a hold of Ks, can he or she decrypt S’s encrypted messages?
Why or why not?
no because they need the corresponding private key to decrypt
4. Are symmetric encryption systems or public key systems better?
public key systems

Lecture 45
1. Why do you suppose most modern symmetric encryption algorithms are block ciphers?
cheaper to compute and save
2. What is the significance of malleability?
jmalleability is bad because the attacker could change the emssage and it would have impact on what it was deciding
3. What is the significance of homomorphic encryption?
homomorphic yuou can link functions together without revealing what the data means.

Lecture 46
1. Which of the 4 steps in AES uses confusion and how is it done?
subBytes. it uses a value as an index for each byte in the array to effectively create a look up table
2. Which of the 4 steps in AES uses diffusion and how is it done?
shiftRows. you shift a given row
3. Why does decryption in AES take longer than encryption?
matrix multiplication is expensive and takes longerse
4. Describe the use of blocks and rounds in AES.
blocks is were data is saved, rounds is in correspondence to the steps you take
5. Why would one want to increase the total number of Rounds in AES?
increaesd confusion and diffusion

Lecture 47
1. What is a disadvantage in using ECB mode?
identical blocks in the plaintext gives the sames on in the ciphertext
2. How can this flaw be fixed?
we randomize the blocks before they are encrypted

3. What are potential weaknesses of CBC?
by observation the attacker will be able ot decipher the first block
4. How is key stream generation different from standard block encryption
modes?
psuedorandom generator

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?
easily coputed but difficult to reverse
3. How do public key systems largely solve the key distribution problem?
increases the time it takes to perform computations
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 more efficient in general becauyse its cheaper

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 it should because they would be equal still, the multiplicative property of exponents
2. Explain the role of prime numbers in RSA.
you can get p1*p2 but it will be hard to factor the result without knowing p1 or p2
3. Is RSA breakable?
yes
4. Why can no one intercepting {M}Ka read the message?
they dont know the private keys
5. Why can't A be sure {M}Ka came from B?
anyone with the Ka could have encrypted it
6. Why is A sure {M}K-1b originated with B?
since we used its public key to decrypt it
7. How can someone intercepting {M}K-1 b read the message?
by having the public key
8. How can B ensure authentication as well as confidentiality when sending a
message to A?
2 pairs of keys, one for private and one for signing and verifying

Lecture 50

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

so you can hash fast and compute the hash just as fast

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

weak: given m1, its harder to find m2 that != m1 if f(m1) = f(m2), no collisions

strong: it is hard to find f(m1) = f(m2)

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

preimage: hard ot find any m such that h=f(m)

second preimage: weak collisions

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

you can brute force is after u calcualte 1.25 ∗(number of combinations)

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

same thing as #4

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

thye are one way

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

it is a one way mapping, there is no backwards

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

yuou can send the hash and the message and then recompute the hash and compare it against what the other person has.

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 R? Why or why not?

no because anyone with the R and S pbulic key can decrypt the message

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?

no difference so yes

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

no

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

to ensure confidentiality and authentication. make it private and make sure the right person gets the message

Lecture 52

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

nothing since it is all known by the eavesdropper

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

they can know a, but they do not know p or g so they cant do anything unless they wanna compute it

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

if thye dont know p and g, they cant do anything with it, they can just use b. same answer a #3 pretty much.