**2024 Semester 1- Tutorial 8 CZ3010 Questions**

1. In the wise man story, at the 20th square, he already had a bag of rice (abt 2^20 grains). How many bags of rice did he earn as his reward?

2^64 / 2^20 = 2^44 wrong

Collect all grains up to 20th square and put it into 1 bag on the 20th square.

Total number of bags(2^20 grains)

1+ 2^1 + 2^2 +…+ 2^44 =~ 2^45 bags of rice

1. (a) Show that the complexity of monoalphabetic substitution (26!) is roughly 2^88. (b)How do you make a monoalphabetic substitution cipher harder to break?
2. 26! = 4.0329x10^26.

2^88 = 3.0949x10^26

First compute log(26!) = log1 + log2 +…+ log26 = 26.606

Call this number X = 26.605

Write 26! = 2^Y

Log(26!) = Y log2 = X

Y = X/log2 = 88.38

1. Instead of shifting all the letters by the same amount, we can scramble the 26 letters into other random permutations
2. A 3GHz PC can crack approximately 2^34 work in 1 day. Calculate the time taken (in years) to crack monoalphabetic substitution by brute force using 1 PC. What about cracking time of 1 billion PCs of same specs?

26! / 2^34 = 2.3475x10^16days = 6.4314x10^13 years

Using 1 PC, cracking time for 2^88 is 2^88/2^34 = 2^54 days = 5 x 10^13 years

1 billion PCs: total per day = 1,000,000,000 x 2^34 = 1.718 x 10^19. Time in years to crack monoalphabetic substitution = 26! / 1.718x10^19/365 = 64314 years

Using 1 billion PCs, takes, 5 x 10^13/10^9 = 50,000 years

Even NSA and big intel cannot crack 88 bit

1. Why do long keywords, shorter message implies stronger Vigenere cipher?

Shorter messages makes it harder to spot patterns in the encrypted text. Longer keywords makes it such that keywords are harder to find and spot.

Long keywords lead to less observable pattern in ciphertext

Also, more frequency tables needed(length n keyword means n different frequency substitution table

Shorter msg means stats analysis not accurate.

1. General Douglas sends the message ATTACK to his soldiers using a one time pad {GZAMCQ} through email. Suppose attacker sniffed out such a ciphertext. Explain why he/she is not able to decrypt this cipher with 100% certainty, assuming attacker knows it’s from a one-time pad.

While the attacker knows that one time pad is used, he can determine the length of the one time pad and the message. However, he does not know the key of the one time pad and has to come out with a list of possible plaintext based on 2^6 possibilities in this case.

Adversary will never be sure if plaintext msg is other meaningful 6 letter word

1. (a) Why must pad be random?

(b) Why must pad be not reused again? (asking for a quantitative reasoning)

a)Making it random makes it such that it cannot be guessed based on previous one time pads.

a) real random pad will ensure perfect secrecy, as each bit has equal chance of 0.5 to appear. Totally unpredictable

b) If used again, the context of the messages or repetition can cause the pad to be decrypted easily.

If pad K is reused

C1 = P1 XOR K

C2 = P2 XOR K

C1 XOR C2 = P1 XOR P2 XOR K XOR K

C1 XOR C2 = P1 XOR P2, K totally disappear

1. Johnny English want to make his OTP encryption even harder for attackers. He decides to encrypt twice using 2 different OTPs. Is his method more secure than the usual one?

Yes, it is more secure than the usual one as even if the attacker decrypts the one OTP, he is not able to tell which decrypted text is from the original text. If the plaintext was 5 characters, the permutation would be 2^5 \* 2^5 = 2^10 wrong

P XOR K1 XOR K2 = P XOR (K1 XOR K2). (K1 XOR K2) is another random string of equal length as K1 and K2. The string is just another same length random string. No extra security if we encrypt with 2 different one time pad

1. NSA has intercepted a Vignere ciphertext: {**Y W W L F F D A Q B H L W B G V G R G S N Z D V U}**, and Ethan Hunt has obtained the key-- **CODE**. **Decrypt this ciphertext.**

Key starts with 0, ciphertext starts with 0(A=0,Z=25)

CODE:2,14,3,4

Ciphertext: 24,22,22,11, 5,5,3,0, 16,1,7,11, 22,1,6,21, 6,17,6,18 ,13,25,3,21, 20

Plaintext: 22,8,19,7, 3,17,0,22, 14,13,4,7, 20,13,3,17, 4,3,3,14, 11,11,0,17, 18

WITHDRAW ONE HUNDRED DOLLARS

1. Use ONLY your mind to create a sequence of 64 random bits, in blocks of 8 bits. Then use any RNG (from OS RNG etc) to generate such a sequence. Then you compare the difference. What are the key things abt the sequence you can expect to observe from a true RNG?

Mind sequence: 10111011 01001001 10110111 10111000 11100011 10100100 01010010 10101011

RNG generator: 01011100 1100 1101 00101011 10011110 00100101 10000001 11011001 01000000

Every bit has an equal probability of being 1 or 0, and that successive bits are independent of each other.

Occurrence of #1 = #0s

Occurrence of #11 = #00 = #01 = #10

00000 roughly same as any other 5 binary characters like 11111

1. In early IPOD days, some listeners complained hearing the same song within 2 hours although they have 400 songs on their ipod. Assuming 4 min songs on average. Question: Is the IPOD shuffling random?

Number of songs within the 2 hours = 2 \*60/4 = 30

Yes, the IPOD is shuffling randomly as every time a song is picked, it could be a song that was played before. To not make the songs repeat so often, there should be random selection on the remaining songs that have not been played yet.

If P(clash) for 30 songs within 400 songs in 2h period >0.5, clash is expected and claims of non randomness might not stand

P(clash) = 1- P(no clash), which is easier to compute

If there were N songs in the IPOD, k songs within period of consideration,

P(no clash) = N/N\*(N-1)/N\*(N-2)/N\*…\*[N-(K-1)]/N

Given N = 400,k=30

P(no clash) = 400/400 \* 399/400 \* … \* 371/400 = 0.327

P(clash) = 0.673, very high chance

Claims of non randomness of IPOD shuffle not justified on this ground

1. Suppose 2 **true** random number generator generates a 8-bit string 11010110 in its first 8 bits & the other generates 00000000 in its first 8 bits. Is the first more random than 00000000?

No. This is as both have equal probabilities to be generated,

Probability = (1/2)^8

Bits required to follow a specific pattern with same probability of occurrence. A number that looks more random is not always so and vice versa