**AY2022/2023 Semester 2- 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. (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?
3. 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?
4. Why do long keywords, shorter message implies stronger Vigenere cipher?
5. 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.
6. (a) Why must pad be random?

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

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?
2. 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 OTP- **CODE**. **Decrypt this ciphertext.**



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. How many 00000 do you expect to find?
2. 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?
3. Suppose 2 random number generates a 8-bit string 11010110 in one portion of the string & another generates 00000000 at another portion. Is the first more random than 00000000?