Amjad Alqahtani
Midterm Exam answers:

1. If all zeros are used, the ciphertext will be identical to the message. For ones, it will be a bitwise complement of the plaintext given that we use XOR. Yes, there will be a risk because it will be predictable. We need randomness and unpredictability.

2. No. The perfect security means Pr[M=m|C=c] = Pr[M=m]. This holds if {every plaintext is mapped to a ciphertext under some key. If we eliminate all zeros, it will not be perfectly secret. This is because the equal probability of different keys does not hold anymore. For the recommendation part, I can recommend a stronger secure key generation scheme that ensures randomness and uniform distribution.

3. The message is hard to assume that they are uniformly distributed. On the other hand, cryptographic security often requires that the key is uniformly selected from the key space.

4. The scheme that achieves perfect security is called a one-time pad. The one-time pad is secure if each key is used to encrypt a single message and the key is as long as the message. Under these conditions, the ciphertext reveals no information about the plaintext, making it unbreakable. If the Vigenere cipher uses a repeating key, it becomes vulnerable to attacks. However, if the key is random and matches the message length, it effectively becomes a one-time pad, but this is not practical.

5. Blocks are 8 blocks and ciphertext length in bits is 1024 bits. Changing in key size will not affect ciphertext length.

6. Yes, this is derived from asymptotic analysis, and it shows that the difference between two negligible functions is also negligible in the asymptotic sense.

7. The indistinguishability states that Pr[Adversary success] <= 1/2 + negl(n). This implies that the adversary's advantage over random guessing is negligible. The first part provides an upper bound on success probability, while the second part shows that adversarial success remains close to random guessing with negligibility.

8. For m and k, the number of possible ciphertexts is 2^n. The explanation is that the r is uniform from $\{0,1\}^n$, which results in 2^n possible values. There will be 2^n for m and k.

9. Encryption is done by using XOR the plaintext with a key generated iteratively from the IV. CTR is a good choice because it supports independent encryption and avoids the sequential dependency of OFB.

10. Security is defined under the assumption that adversaries are probabilistic polynomial-time algorithms. With restriction, we will maintain the practicality of computational complexity assumptions and prevent adversaries from gaining unrealistic computational power.

11. CTR is resilient to dropped ciphertext blocks while CFB suffers from error propagation, making it less robust.

12. Dropped blocks do not break overall decryption while Bit-flipping can be exploited for malicious tampering and makes CBC vulnerable to attacks. To prevent bit-flipping attacks, CBC should be used with authenticated encryption schemes.