MATH 3540 **Name:** ____________________

Midterm

Directions

1. Complete the following questions.

---

1. Using the English-language shift cipher which of the following plaintexts could correspond to ciphertext ”qzhpd”

   (a) ”pygoc”

   (b) ”bad”

   (c) ”lucky”

   (d) ”tough”

2. Which of the following encryption schemes are perfectly secret ?

   (a) shift cipher

   (b) vigenere cipher

   (c) Psuedo-one time pad

   (d) one time pad

3. Consider the vigenere cipher where the key space and message space are all single english words of length 3 composed of only lowercase letters. What is the probability that key k is equal to ’abc’?

   (a) $(1/25)^3$

   (b) 1/5

   (c) 1/26

   (d) None of the above

4. Which of the following is NOT a drawback of the one-time pad?

   (a) A given key can only be used to encrypt one message

   (b) The key is as long as the message

   (c) The key must be chosen uniformly

   (d) The scheme is insecure against chosen-plaintext attacks

5. Which of the following is a negligible function?

   (a) $f(n) = 1/n$

   (b) $f(n) = 1/2$

   (c) $f(n) = 1/2^n$

   (d) $f(n) = n/2^n$

6. Define G by G(x) = $x|x$. (G maps inputs of length n to outputs of length 2n.) Which of the following algorithms A distinguishes the output of G from uniform?

   (a) An input y of length 2n, output 1 if the first bit of y is 1

   (b) An input y of length 2n, output 1 if the last bit of y is 1

   (c) An input y of length 2n, output 1 if the first and last bits of y are equal

   (d) An input y of length 2n, output 1 if the first bit of y is equal to the (n+1)st bit of y

7. Consider the one-time pad over the message space of 6-bit strings, where Pr[M=001000] = 0.15, Pr[M=110011] = 0.25, and Pr[M=111111] = 0.6. Note that the key space consists of any 6 bit string. What is Pr[C=000000]?

8. Prove or refute: There exists a perfectly secret encryption scheme Π with message space M and key space K such that $|M| > |K|$.

9. Prove or refute: If a single character is encrypted, then the shift cipher is perfectly secret.

10. Let G be a pseudorandom generator and define $G_0(s)$ to be the output of G truncated to n bits (where s is of length n). Prove that the function $F_k(x) = G_0(k) \bigoplus x$ is not a pseudorandom function.

11. Show that the pseudo-OTP is not CPA secure.

12. Let $\pi = (Gen; Enc; Dec)$ be an encryption scheme defined as follows where F is a pseudorandom function:

    (a) Gen: On input 1^n, Gen ouputs a key $k \in \{0,1\}^n$ choosen uniformly .

    (b) Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose a string $r \in \{0,1\}^n$ uniformaly and output the ciphertext

    $$c =< r, F_k(r) \bigoplus m > .$$

    (c) Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext c =¡r,s¿, output the message

    $$m = F_k(r) \bigoplus s.$$

    Show correctness of π.

13. Let $(Gen; Enc; Dec)$ be an encryption scheme defined as follows:

    (a) Gen outputs a key k for a keyed function F.

    (b) Upon input $m \in \{0,1\}^{n/2}$ and key k, algorithm Enc chooses a random string $r \leftarrow \{0,1\}^{n/2}$ of length $n/2$ and computes $c = F_k(r|m)$.

    Show the following:

    (a) Define the decryption algorthim for π.

    (b) If F is a random permutation show π is CPA secure.

    (c) If F is a psuedorandom permutation show π is CPA secure.