1. Which of the following functions are negligible?
    a. $n^{100}n^{-\log(n)}$
    b. p(n)f(n), if f(n) is a negligible function and p(n) is a polynomial
    c. $1/n^{100}$
    d. 1/2n
    e. 2^n

Answer=a,b

2.Which of the following functions are negligible?
    a. $1/1000n^4 + n^2\log(n)$
    b. f(n)-g(n), if f(n) is non-negligible and g(n) is negligible
    c. $3^{-\sqrt{n}}$
    d. 1/n
    e. 1/2

Answers=c

1. Which of the following functions are not negligible?
    a. 2^{-n}
    b. $2^{-c\log(n)}$ for positive c.
    c. $2^{-\sqrt{n}}$
    d. f(n)+g(n), if f(n) and g(n) are negligible functions
    e. $2^{-n}+2^{-\sqrt{n}}$

Answer= b

Q - Let *f* be a **negligible function**. Defining below the overwhelming and noticeable functions:

Overwhelming function: A function is *f* is overwhelming if 1-*f* is negligible.

Noticeable function: A positive function *f* is noticeable if there exist a positive polynomial p and a number n_0 such that *f(n)>=1/p(n)* for all $n>=n_0$.

Now, consider the function Z(n):=1 for even and $Z(n):=2^{-n}$ for odd.

Then Z is? (Tick all those whose definition Z follows)

A) Negligible function

B) Overwhelming function

C) Noticeable function

D) Z is neither Negligible, Overwhelming nor Noticeable

Ans) D

1. Which one of these are commonly used methods to break substitution ciphers?
    - Reverse Substitution
    - Frequency Analysis
    - Man In The Middle Attack
    - Brute Force Attack

Q - Assume that there exists a new variant of the ROT-8 substitution, called the ROT{X}-8, where it is possible to shift the characters in the message string 8 places forward by a probability of 0.6, and 8 places backwards by a probability of 0.4 (so, if the character is A, the probability of it becoming I is 0.6 and the probability of it being S is 0.4). Assuming that you apply this new ROT{X} - 8 substitution on the plaintext 10 times, what is the probability of the plaintext and the ciphertext being the same? The length of the plaintext is 5.

- Numerical value answer

Q - Define a scheme K as follows - We apply ROT-X on plaintext 26 times, where X $\in \{1, 2, 3, \dots, 26\}$. So we apply ROT-1 first, then ROT-2, then ROT-3, … ROT-26. Given the plaintext is “BLUEPRINTS”, what is the ciphertext?

Q - In Shannon’s equation, M equally likely messages, $M >> 1$, if the rate of information $R > C$, the probability of error is

a. Arbitrarily small
b. Close to unity
c. Not predictable
d. Unknown

Q. Consider the one-time pad over the message space of 6-bit strings, where $Pr[M = 001000] = 0.1$ and $Pr[M = 110111] = 0.9$. What is $Pr[C = 000000]$?

a. 0.03125
b. 0.03333
c. 0.15625
d. 0.16667

Q. Assume that hc(x) is the hardcore predicate of one-way function f(x), where x ← {0, 1}*. It is given that Pr[A(f(x) = hc(x)] <= ½ + g(n), where g(n) is any function on the value n. Tick all

possible choices for g(n). [if including this question in the test set, remove first question from negligible functions]

- **2^(-n)**
- **1/n^2**
- **n/n!**
- **1/log(n)**

Q-Define g(x,r) = (f(x), r), where both x,r ← {0, 1}* - this means that, applying g on x and r is the same as applying f() on x (using r) whilst keeping r unchanged. Under what conditions will the bit $\oplus x_i.r_i$ be a hardcore predicate?

- **|x| = |r|, f(x) = x^2 mod n, where n = p x q, and both p and q are prime.**
- **|x| ≥ |r|, f(x) = g^x mod p, where p is prime, g is generator of the multiplicative group Z_p.**
- **|x| ≤ |r|, f(x) = x^2 mod n, where n = p x q, and both p and q are coprime.**
- **|x| > |r|, f(x) = g^x mod p, where p is prime, g is generator of the multiplicative group Z_p.**

Q1:- Let F: $\{0,1\}^n * \{0,1\}^n$ be a secure PRF, where key space, input space and output space are all $\{0,1\}^n$, and n=128. Which of the following is secure PRF ?

1. F' (k,x) = F(k,x) ⊕ F(k, x ⊕ 1^n)
2. F' ((k_1,k_2),x) = {F(k_1,x), when x ≠ 0^n
   k_2 , otherwise. }
3. F' ((k_1,k_2),x) = {F(k_1,x) || F(k_2, x)
4. None of these

Ans:- 2,3

---

13) Given two MAC schemes, out of which one is strongly secure, and the other is not strongly secure, how would one go about

creating a new MAC scheme that is strongly secure? Notice that you do not know which one of the two schemes are strongly secure.

1. Take individual bits of both the output tags and bitwise AND them to produce the output.
2. Take individual bits of both the output tags and bitwise OR them to produce the output.
3. Take individual bits of both the output tags and bitwise XOR them to produce the output.
4. Concatenate both the output tags into a new tag.

14- The CCA indistinguishability experiment $PrivK_{A,\Pi}^{cca}(n)$:

a. A key k is generated by running $Gen(1^n)$.
b. The adversary A is given input 1^n and oracle access to $Enc_k(\cdot)$ and $Dec_k(\cdot)$. It outputs a pair of message m_0, m_1 of the same length.
c. A random bit $b \leftarrow \{0,1\}$ is chosen, and then a ciphertext $c \leftarrow Enc_k(m_b)$ is computed and given to A. We call c the challenge ciphertext.
d. The adversary A continues to have oracle access to $Enc_k(\cdot)$ and $Dec_k(\cdot)$, but is not allowed to query the latter on the challenge ciphertext itself. Eventually, A outputs a bit b'.
e. The output of the experiment is defined to be 1 if b'=b, and 0 otherwise.

Jumble the above steps and ask students to arrange them in order of CCA indistinguishability experiment.

15 - Which of the following are good candidates for a one-way function?

a. f (p, q) = pq, for randomly chosen primes p,q
b. $f(x) = x^2$
c. If $f:\{0,1\}^n \rightarrow \{0,1\}^n$ is a one-way function, then $g:\{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ defined as $g(x) = 0_n || f(x_{[1:n]})$.
d. Identity function f(x)=x.

answer= a,c.

16) In class, the 4 basic modes of operations of block ciphers (ECB, CBC, OFB, Counter) are analyzed w.r.t. consequence on ciphertext blocks by changing a single plaintext block are discussed.

For all 4 modes of operation, analyze the effect on the decryption of remaining blocks if for the sequence of ciphertext blocks $c_1,c_2,..,c_n$ some ciphertext block c_j is error $1 \leq j < n$.

Specify which of plaintext blocks x_j , x_{j+1}, $x_{j+2},\ldots,x_n$ are received correctly.

Assume ciphertext c_1 is incorrect.

1) **For ECB mode:**
   a) Only x_1 is decrypted incorrectly
   b) Only x_1,x_2 are decrypted incorrectly
   c) Only x_1,x_2,x_3 are decrypted incorrectly
   d) All blocks are decrypted incorrectly.

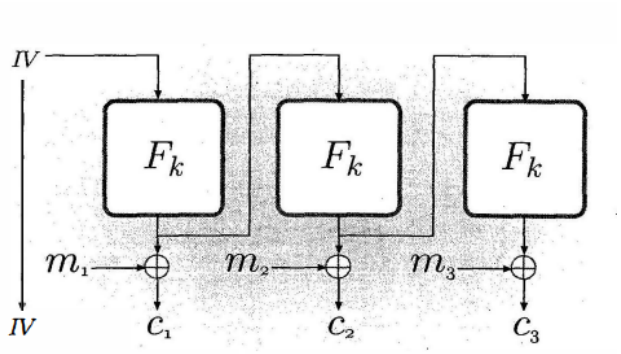
   Ans) a

2) **For CBC mode:**
   a) Only x_1 is decrypted incorrectly
   b) Only x_1,x_2 are decrypted incorrectly
   c) Only x_1,x_2,x_3 are decrypted incorrectly
   d) All blocks are decrypted incorrectly.

   Ans) d

17)

1)Identify the mode of operation in the below diagram:



a) CBC mode
b) CTR mode
c) ECB mode
d) OFB mode

Ans) d

18 - Which of the following statements are true

(a) Kerckhoff's principle asks us to never reveal the encryption algorithm
(b) Caesar cipher follows the Kerckhoff's principle
(c) Every algorithms that follows Kerckhoff's principle is secure
(d) Caesar cipher does not follow the Kerckhoff's principle

ANS: (d)

19 - Generalizing the computation of LSB(x), given g^x mod p, which of the following is true?

(a) If m divides (p-1),It is possible to compute x mod m in O(m polylog p) time
(b) It is easy to solve DLP if (p-1) does not have a prime factor greater than polylog(p)
(c) DLP for Fermat primes (primes of the form $2^k + 1$) are always easy
(d) Therefore, it is best to choose p such that (p-1)/2 is a prime too

ANS: a,b,c,d

20 - Assuming that DLP is hard for p=19, g=2, and MSB(x) is its hard-core predicate, what are the first few bits output by a PRG designed from the above for the seed/key 5:

(a) 0 1 0 0 …
(b) 0 0 1 1 …
(c) 0 1 1 0 …
(d) 0 1 0 1 …

ANS (a)

21 - An attack on basic CBCMAC requires:

(a) Tags for two messages of same length
(b) Tags for millions of messages of same length
(c) Tags for any two messages of different lengths
(d) Tags for specifically chosen two messages of different lengths

ANS (d)

22 - Given a CPA-secure encryption scheme and a secure MAC scheme, it is easy to design a CCA-secure encryption scheme as follows:

(a) Authenticate the message and then encrypt the outcome
(b) Encrypt the message and then authenticate the ciphertext
(c) Separately encrypt the message and authenticate the message

(d) The key trick is to use the same secret key for both encryption and authentication

ANS (b)