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

Answer= a,c,e

2. 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

3. Which of the below statements are true?

    A) If f is negligible, then for any c, $f^c$ is negligible.

    B) If f is negligible, then cxf is negligible for any non-zero constant c.

    C) If f1 and f2 are negligible, then f1-f2 is not always/necessarily negligible.

D) If f is negligible and p is polynomially bounded (i.e. there is a positive polynomial r that is bigger than p for sufficiently large n), then p.f is negligible.

**Ans) C, D**

4. Though discrete logarithm may be hard, computing the logarithm modulo 2 is easy, that is, given $y = g^x \bmod p$, x mod 2 is got by computing the following (modulo p):
   a. $y^p$
   b. $y^{[(p+1)/2]}$
   c. $y^{[(p-1)/2]}$
   d. $y^y$

   ANS: C

5. What is x mod 2, given that $2^x \bmod 19 = 13$? It is:
   (a) 0 if $13^9 \bmod 19$ is 1 and 1 if $13^9 \bmod 19$ is 18
   (b) 0 if $2^9 \bmod 19$ is 1 and 1 if $2^9 \bmod 19$ is 18
   (c) 0 if $2^{13} \bmod 19$ is 1 and 1 if $2^{13} \bmod 19$ is 18
   (d) 0 if $2^9 \bmod 19$ is 18 and 1 if $2^9 \bmod 19$ is 1

   ANS: (a)
6. Which of the following ciphertexts can be formed by applying a standard ROT-13 substitution cipher on the plaintext “CYBERPUNKS”?
7. Consider a vigenere cipher over the set {a, b, c, … , m} ∪ {N, O, P, Q, … , Z}. The length of the key, L ∈ {5, 6, 7, 8, .. , 12}. What is the size of the key space for this scheme? Select all the options that apply.
   - 26 * ( $\sum_{k=5}^{12} k$)
   - 26 ^ ( $\sum_{k=5}^{12} k$)
   - 26^5 + 26^6 + 26^7 + … + 26^12
   - $\sum_{k=5}^{12}$ 26^k

Consider the following statements. Choose the correct ones.

a. Consider a cryptosystem in which $P = \{a, b, c\}$, $K = \{K_1, K_2, K_3\}$ and $C = \{1, 2, 3, 4\}$. Suppose encryption matrix is as follows:

| | a | b | c |
|---|---|---|---|
| K1 | 1 | 2 | 3 |
| K2 | 2 | 3 | 4 |
| K3 | 3 | 4 | 1 |

This system has perfect secrecy.

b. Every encryption scheme for which the size of the key space equals the size of the message space and for which key is chosen uniformly from the key space is perfectly secret. True or False ?

c. An encryption scheme (Gen, Enc, Dec) over a message space M is perfectly secret if and only if every probability distribution over M, every $m_0, m_1 \in M$, and every $c \in C$:
$Pr[C = c \mid M = m_0] = Pr[C = c \mid M = m_1]$

8.

9. - 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

10. -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: Enter first 4 bits (ans = 0100)

11. -Let G:K -> $\{0,1\}^n$ be a secure PRG. Define G'(K1,K2)=G($K_1$) & G($K_2$) where & is bitwise AND. consider following statistical test A on $\{0,1\}^n$ : A(x) outputs LSB(x) , LSB stands for least significant

bit) what is $Adv_{PRG}[A,G']$ ? Assume that LSB(G(k)) is 0 for exactly half the seeds k in K.

Answer: 0.25

12. -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 not secure PRF ?

1. $F'(k,x) = F(k,x) \oplus F(k, x \oplus 1^n)$
2. $F'(k,x) = \{F(k,x)[0,...,n-2]$, i.e $F'$ drops last bit of F
3. $F'(k,x) = \{F(k,x)$, when $x \neq 0^n$
   k, otherwise. }
4. None of these

   Ans:- 1,3

13. - Let $R := \{0,1\}^4$ and consider the following PRF

F: $R^5 \times R \rightarrow R$ defined as follows:

```
F(k,x): { t = k[0]
          For i=1 to 4 do
              if(x[i-1)==1) t = t ⊕ k[i]
          Output t
}
```

(i.e.)key K = (k[0], k[1], K[2], k[3] ) in $R^5$ .

For eg: function at 0101 is defined as $F(k,0101) = k[0] \oplus k[2] \oplus k[4]$.

For some random key unknown to you, you learn that F(k,0110) = 0011 and F(k,0101) = 1010 and F(k,1110) = 0110. What is the value of F(k,0011) ?

Ans:- Numerical type (1111)

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 ← {0,1} is chosen, and then a ciphertext c ← $Enc_k(m_b)$ 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 statement is true :-

1) Any CPA-Secure system must be deterministic because no probabilistic encryption scheme can be secure against chosen-plaintext attacks.
2) Any CPA-Secure system can be deterministic or probabilistic because both deterministic and probabilistic encryption schemes can be secure against chosen-plaintext attacks.
3) Any CPA-Secure system must be probabilistic because no deterministic encryption scheme can be secure against chosen-plaintext attacks.
4) None of these.

Ans:-3

16. -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)

17. -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.

18. -Assume a MAC scheme with keyspace k and tag space t. Suppose that the size of the key space is K and the size of the tag space is T. What is the overall number of iterations required to break the MAC scheme using brute force with linear search?

1. max(2^K, 2^N)
2. min(2^K, 2^N)
3. 2^(K + N)
4. 2^(K * N)

19. -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)

20. -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**

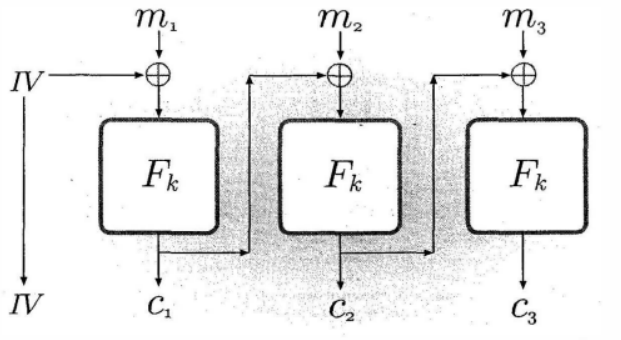
3) **For OFB mode:**
   a) Only $x_1$ is decrypted incorrectly
   b) Only $x_1$,$x_2$ are decrypted incorrectly
   c) Only $x_1$,$x_2$,$x_3$ are decrypted incorrectly
   d) All blocks are decrypted incorrectly.

**Ans) a**

4) **For CFB 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**

21. -Identify the mode of operation in the below diagram:




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

**Ans) a**

22. -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

23. -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

24. -**Define g(x,r) = (f(x), r), where both x,r $\leftarrow$ {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| $\geq$ |r|, f(x) = g^x mod p, where p is prime, g is generator of the multiplicative group $Z_p$.**
- **|x| $\leq$ |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 $Z_p$.**