Q1) Which of the following functions are not negligible?

a. f(n)-g(n), if f(n) is non-negligible and g(n) is negligible
b. 2^{-n}
c. $n^{-\log(n)}$
d. $1/(1000n^4 + n^2\log(n))$
e. $2^{-n}+2^{-\sqrt{n}}$

Answer= a,d

Q2) 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

Q3) Identify all the statements which are true:

A) A positive function f(n) is negligible iff for any positive polynomial p(n) the product p(n)f(n) converges to 0.

B) A positive function f(n) is negligible iff for any positive polynomial p(n) the product p(n)f(n) converges to 1.

C) A positive function f(n) is negligible iff for any natural number i the product n^i * f(n) converges to 0.

D) A positive function f(n) is negligible iff for any natural number i the product n^i * f(n) converges to 1.

Ans) A, C

Q4) Analogous to the ease of computing discrete logarithm mod 2, suppose that 3 divides p-1, one may compute x mod 3, given $y = g^x$ mod p by computing the following (modulo p):

(a) $y^{(p-1)/2}$
(b) $y^{[(p+2)/3]}$
(c) $y^{[(p-1)/3]}$
(d) y^y

ANS: C

Q5) What is x mod 3, given that 2^x mod 19 = 13?

(a) 0 if 13^6 mod 19 is 1, 1 if 13^6 mod 19 is 7 and 2 if 13^6 mod 19 is 11
(b) 0 if 2^9 mod 19 is 1, 1 if 2^9 mod 19 is 18 and 2 if 2^9 mod 19 is 11
(c) 0 if 2^{13} mod 19 is 1, 1 if 2^{13} mod 19 is 11 and 2 if 13^6 mod 19 is 7
(d) 0 if 2^9 mod 19 is 18 , 1 if 2^9 mod 19 is 1 and 2 if 2^9 mod 19 is 13

ANS: (a)

Q6) Given that we're applying the ROT-13 algorithm on the plaintext "NHGUBEVMR" an odd number of times, and then applying ROT-6 and ROT-7 algorithm (together, in that order) an even number of times, what will be the final ciphertext?
Ans) AUTHORIZED

Q7) For a vigenere cipher over a set of 5 strings that are of the length 4, we define the key space as follows - The probability of choosing a string of length k is defined by $1/2^k$, where k $\in N$. Assume that the character space used for

creating the message strings and their corresponding key strings is infinite in size, i.e, inexhaustible and that all the message/key strings are unique. What is the probability of constructing a perfectly secure scheme with this set up?

This is the answer: 3.05 * 10 ^ (-5)

Q8) Let (Gen, Enc, Dec) be an encryption scheme over a message space M from which $|M|$ = |K| = |C|. The scheme is perfectly secure if and only if:

a. Every key $k \in K$ is chosen with equal probability $1/|K|$ by algorithm Gen.
b. Some key $k \in K$ is chosen with equal probability $1 / |K|$ by algorithm Gen.
c. For every $m \in M$ and every $c \in C$, there exists a unique key $k \in K$ such that $Enc(m)$ outputs c.
d. There does not exists a unique key $k \in K$, for every $m \in M$ and every $c \in C$ such that $Enc(m)$ outputs c.

Q9) 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

Q10) 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)

Q11) Let G:$\{0,1\}^s$ -> $\{0,1\}^n$ be a secure PRG. Which of the following is secure PRG?

A) $G'(k_1,k_2)=G(k_1) \,||\, G(k_2)$
B) $G'(R)=G(0)$

C) G'(k)=G(k) || G(k)
D) G'(k)=G(k) || 0
E) G'(k)=G(k xor 1^s)
F) G'(k)= reverse(G(k)) [reverse() -> reverse the string]

Q12) 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. $F'(k,x) = \{F(k,x)$, when $x \neq 0^n$
   0^n , otherwise. }
2. $F'(k,x) = \{F(k,x)[0,...,n-2]$, i.e F' drops last bit of F
3. $F'((k_1,k_2),x) = \{F(k_1,x) \| F(k_2, x)$
4. None of these

Ans:- 2,3

Q13) 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]⊕k[2]⊕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,1111) ?

Ans:- Numerical type

Q14) The CPA indistinguishability experiment $PrivK_{A,\Pi}^{cpa}(n)$:

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 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 outputs a bit b'.
e. The output of the experiment is defined to be 1 of b' = b, and 0 otherwise.(In case $PrivK_{A,\Pi}^{cpa}(n)=1$, we say that A succeeded.)

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

Q15) Which of the following is true:-

1) Any cipher that prevents chosen-plaintext attacks is also secure against known-plaintext and ciphertext-only attacks
2) Any cipher that prevents known-plaintext attacks is also secure against chosen-plaintext and ciphertext-only attacks.
3) Any cipher that prevents chosen-plaintext attacks is not secure against known-plaintext and ciphertext-only attacks.
4) None of these

Ans: 1

Q16) Secure MACs guarantee that:

(a) No adversary (including unbounded ones) can forge a new message and its valid tag
(b) No efficient adversary can forge a new message and its valid tag with a non-negligible chance
(c) Replay attacks are thwarted
(d) None of these

ANS (b)

Q17) For an x bit key and a y bit tag, the maximum level of effort required for brute force attack on CBC-MAC algorithm is?

A) 2^x
B) 2^y
C) $\max(2^x,2^y)$
D) $\min(2^x,2^y)$
E) $2^{(x+y)}$

Q18) 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.

Q19) Encrypt-and-then-Authenticate using a CPA-secure encryption scheme and a secure MAC scheme results in:

(a) A CCA-secure encryption scheme if the same keys are used for both encryption and authentication

(b) A CCA-secure encryption scheme if independently chosen keys are used for encryption and authentication

(c) A potentially insecure encryption scheme if the same keys are used for both encryption and authentication

(d) An encryption scheme that is certainly/surely insecure if the same keys are used for both encryption and authentication

ANS (b) and ©

Q20) Alice and Bob use a block cipher for encryption and need to choose a mode of operation out of CBC and Counter Mode. An adversary is able to intercept and changes the messages sent between Alice and Bob. Now consider the following scenarios:

1. In some messages sent by Bob, it is the case that the last block of message is a secret key. Decide for the two modes whether the adversary can corrupt messages sent, so that Alice receives a message that looks good after decryption, but contains the wrong key.

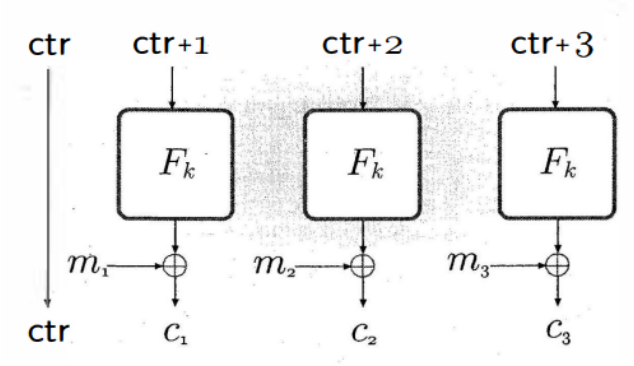
a. Only in CBC mode but not in Counter mode, the adversary can corrupt.

b. For both modes it is the case that the adversary can replace the last cipher-text block with any other block.
c. Only in Counter Mode but not in CBC mode, the adversary can corrupt.
d. Both modes are secure from the attack.

2. In some messages sent by Bob, the adversary may know the first block M1 and want to replace it by another block A1 of his choice, leaving the rest of the message unchanged.

a. This attack is possible in only Counter Mode and not in CBC mode.
b. This attack is possible in both Counter and CBC Mode.
c. This attack is possible on CBC Mode only by assuming C_0 = IV.
d. Both modes are secure from the attack

Q21) Identify the mode of operation in the below diagram:



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

Ans) b

Q22) 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

Q23) 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

Q24) 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 $\bigoplus x_i.r_i$ 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.**

.