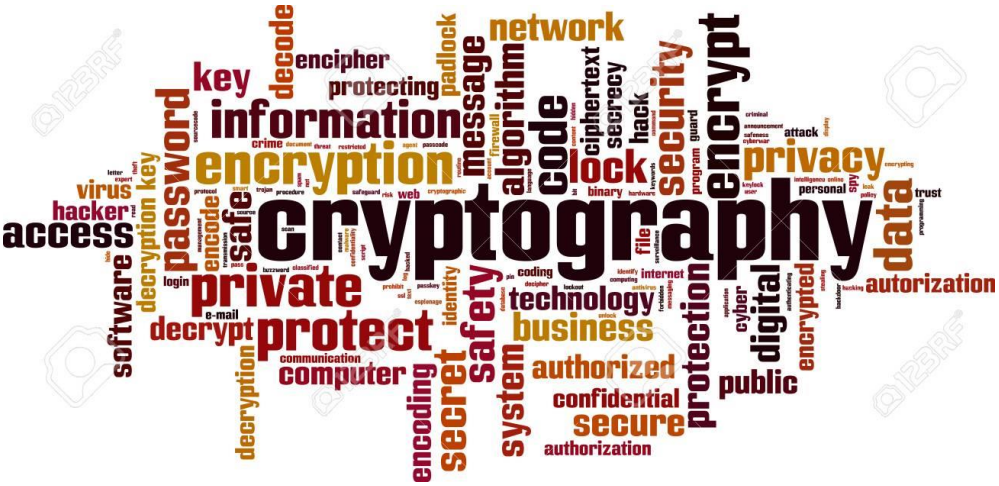
CRYPTOGRAPHY

CSPC-35



09/05/2021

Assignment - 3

Submitted By: -

106118085 - Sampurn Anand

106118105 - Manvitha Vunnam

106118115 - Sabrina Rahman

106118073 - Pavitra Visvanatharoa

106118027 - Raja Yadidiah

Assignment - 3

1) What is one-way function? What is trapdoor one-way function?

Ans → **One-way function :**

$f(x) \to y$ is one way function if given x, it takes polynomial time to find $f(x)$ but for given y, it is very hard to find x such that $f(x) = y$.

Trapdoor One-way function :

$f(x) \to y$ is trapdoor one-way function, if for given x, it is easy to find $f(x)$ but for given y, it is hard to find y such that $f(x) = y$ without trapdoor (secret) but easy to find x such that $f(x) = y$ with trapdoor.

2) State and prove the correctness of RSA crypto-system.

Ans →

RSA crypto-system :

- **Encryption :**
  Enc $(m, e, c) \Rightarrow c = m^e \bmod n$ — (i)
- **Decryption :**
  Dec $(c, d) \Rightarrow m = c^d \bmod n$ — (ii)

Combining (i) and (ii) :-

$m = (m^e \bmod n)^d \bmod n$

$\Rightarrow m = m^{ed} \bmod n$

$\therefore$ To prove :- $m = m^{ed} \bmod n$ — (A)

Proof :- $\because ed = e_1 \bmod \phi(n)$

$\Rightarrow ed = K * \phi(n) + 1$

(A) $\Rightarrow m^{K\phi(n)} \bmod n = 1$

Now,

$Z_n = \{x : \text{GCD}(x, n) = 1\} \bmod n$ is a group. $\Rightarrow |Z| = \phi(n)$

Also, order of an element 'a' divides the number of elements in that group.

Let $o(a) = e$ for $a \in Z_n$, where 'e' is least positive integer such that

$a^e \bmod n = 1$

$\Rightarrow e$ divides $\phi(n)$

If $m \in Z_{n^*}$, $m = p, 2p, 3p, \ldots, q\phi(n)$
$mk = q, 2q, \ldots, kq$

If $a^x \bmod n = 1 \Rightarrow m^{k \cdot \phi(n)} \bmod n = 1$ if $m \in Z_{n^*}$

Let $m = kp$ where $k = \{1, 2, \ldots, q\}$
Using Fermat's Theorem,

$$m^{q-1} \bmod q = 1$$
$$\Rightarrow m^{(p-1)(q-1)k} \bmod q = 1$$
$$\Rightarrow m^{k\phi(n)} = 1 + sq, \text{ where } s = \text{quotient}$$
$$m^{k\phi(n)+1} = m + msq = m + sq(kp)$$

$$(m^{k\phi(n)+1}) \bmod n = m \bmod n + (skn) \bmod n = m \bmod n$$
$$= m \quad (\text{if } m < n)$$
$$\Rightarrow m^{k\phi(n)} \bmod n = 1$$

Hence, proved.

3) Find the computational cost (in terms of bit operations) of key generation in RSA algorithm.

Ans → $t(n) = O(\log n) + O(c) + O(c) + O(\log n) + O(\log n)$

- $O(\log n)$: Choosing p & q
- $O(c)$: Calculating n
- $O(c)$: Calculating $\phi(n)$
- $O(\log n)$: Calculating gcd $(e, \phi(n))$
- $O(\log n)$: Calculating d

4) For RSA with parameters $e = 7$ and $n = 17 * 31$

a) Encrypt the message block $M = 2$.

Ans → $c = m^e \bmod n$
$= 2^7 \bmod 17 * 31$
$= 128$

b) Compute a private key corresponding to given above public key.

Ans → $n = 17 * 31 = 527$, $e = 7$, $\phi(n) = 16 * 30 = 480$
$d = e^{-1} \bmod \phi(n) = 7^{-1} \bmod 480$ #
7 and 480 are coprimes. $\Rightarrow 7p + 480q = 1$
Here, $q = 7^{x} \bmod 480$ and $p = 7^{-1} \bmod 480$
Applying Euclidean algorithm :-

$480 = 7 \cdot 68 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$\Rightarrow 1 = 4 - 3.1$

$= 4 - (7 - 4.1)$ $= 2.4 - 7$

$= 4.4 - 7.3$ $= 2.(480 - 7.68) - 7$

$= 4.(480 - 7.68) - 7.3 = 2.480 - 7.137$

$= 4.480 - 7.\cancel{69}275$

$\therefore q = 42$ and $p = -137$

$\Rightarrow 7 \cancel{\text{mod}} \bmod 480 = 2$ and,

$7^{-1} \bmod 480 = -137$

$\therefore \phi(n) = 7^{-1} \bmod 480 = -137 = -137 + 480$

$\phi(n) = 343$

c) Perform the decryption of obtained cyphertext using the method which is 4x faster than usual method (using CRT).

Ans → Using CRT,

$m = c^d \bmod n$

$= (128)^{343} \bmod 527 = (128)^{343} \bmod (17 * 31)$

$x_p = 128^{343 \bmod (17-1)} \bmod 17$

$= 128^{343 \bmod 16} \bmod 17$

$= 128^{7 \bmod 16} \bmod 17$

$= (2^7)^{7 \bmod 16} \bmod 17$

$= 2^{489 \bmod 16} \bmod 17$

$x_p = 2^{17} \bmod 17$

$x_q = (128)^{343 \bmod (31-1)} \bmod 31$

$= (128)^{343 \bmod 30} \bmod 31$

$= 128^{13 \bmod 30} \bmod 31$

$= (2^7)^{13 \bmod 30} \bmod 31$

$= 2^{91 \bmod 30} \bmod 31$

$= 2^1 \bmod 31$

$c^d \bmod pq = (2 * 31 (q^{-1} \bmod p) + 2 * 17 (p^{-1} \bmod q)) \bmod pq$

17 & 31 are coprimes.

$31 = 17 \cdot 1 + 14$

$17 = 14 \cdot 1 + 3$

$14 = 3 \cdot 4 + 2$

$3 = 2 \cdot 1 + 1$

$\Rightarrow 1 = 3 - 2 \cdot 1$

$= 3 - (14 - 3 \cdot 4)$

$= 3 \cdot 5 - 14$

$= (17 - 14) \cdot 5 - 14$

$= 17 \cdot 5 - 14 \cdot 6$

$\therefore q^{-1} \bmod p = 5$ and $p^{-1} \bmod q = 6$

$\therefore c^d \bmod pq = (2 * 31 * 5 + 2 * 17 * 6) \bmod 527$

$= (320 + 205) \bmod 527$

$= 525 \bmod 527$

$= 2$

5) Let N be a product of 2 primes. Prove formally that hardness of factorization of N implies hardness of finding $\phi(N)$ given N.

Ans ⇒ Let $N = p * q$ where p, q are primes.

$\Rightarrow \phi(N) = \phi(p) * \phi(q) = (p-1) * (q-1)$

↓

Computation takes $O(1)$ time if p, q (factorization of N) is known.

Hence,

if N can be factorized as product of 2 primes then, $\phi(N)$ can be found easily in $O(1)$ time.

∴ If factorizing N takes $O(f(N))$ time, then calculating $\phi(N)$ takes $O(f(N)) + O(1) = O(f(N))$ where $f(N)$ is non-deterministic time.

Based on these calculations, it can be stated that: Hardness of factorization of N implies hardness of finding $\phi(N)$ for given N.

6) Let (N, e) be an RSA public key. Given the private key d, show that one can efficiently factor the modulus N.

Ans :-) Public key = (N, e)

Private key = d

Let p & q be 2 large prime numbers

$$N = pq$$

$$\phi(N) = \phi(pq) = (p-1)(q-1) = N - (p+q) + 1$$

$$d = e^{-1} \bmod \phi(N)$$

$$\Rightarrow ed = 1 \bmod \phi(N)$$

$$\Rightarrow ed - 1 = \text{a multiple of } \phi(N)$$

Let g be randomly chosen from $[2, N-1]$,

$$x = 1 \text{ and } K = ed - 1 = 2^{*} s$$

while $(x == 1)$ {

compute $x = g^{K/2} \bmod N$ and set $K = K/2$ }

$\therefore$ $\gcd(x-1, N) = p$ and $q = N/p$

Thus, the modulus N can be efficiently factored.

(7) Let e_a and e_b be the public keys of the two encryption schemes by Charles.

For the common message m,

$$C_a = m^{e_a} \bmod n$$

$$C_b = m^{e_b} \bmod n$$

Now as we know that $GCD(e_a, e_b) = 1$, so by extended euclidean algorithm, we have some integers p and q such that $p * e_a + q * e_b = 1$

As e_a and e_b are public, adversary finds the value of p and q corresponding to the above equation.

$$C_a^p * C_b^q = (m^{p*e_a} \bmod n) * (m^{q*e_b} \bmod n)$$

$$= (m^{p*e_a + q*e_b} \bmod n)$$

$$= m^1 \bmod n$$

$$= m \bmod n$$

Assuming $m < n$, we get

$$m = C_a^p * C_b^q$$

Hence, the adversary can find the value of m from the values of C_a and C_b and p and q from above.

(8) We can rewrite the given equation as follows:

$$(x+2)^2 \equiv 3 \bmod 23$$

We now replace $(x+2)$ ~~with~~ with y.

$\Rightarrow$ We get $y^2 \equiv 3 \bmod 23$

$$y^2 \equiv 3$$

After solving the equation, we find that the value of y is either 7 or 16.

If $y = 7 \Rightarrow x = 5$

If $y = 16 \Rightarrow x = 14$

(9) Let $2^{1/11} \bmod 19 = m$

comparing the above equation with the RSA equation $C = m^e \bmod n$

we get,

$C = 2, e = 11, n = 19$ and we need to find m

we use $m = c^d \bmod n$ to find m where

$d = e^{-1} \bmod \phi(n)$

$d = 11^{-1} \bmod \phi(19)$

$d = 11^{-1} \bmod 18$

$d = 5$

$m = 2^5 \bmod 19$

$= 32 \bmod 19$

$\Rightarrow m = 13$

(10) ~~$x \equiv 12 \pmod{25}$~~

~~$\Rightarrow 12 = x + 25q$ for some integer q~~

(10) We take $a_1 = 12, a_2 = 9, a_3 = 23$

and $n_1 = 25, n_2 = 26, n_3 = 27$

So $N = 25 * 26 * 27 = 17550$

$N1 = \frac{17550}{25} = 702$

$N2 = \frac{17550}{26} = 675$

$N3 = \frac{17550}{27} = 650$

Applying the chinese remainder theorem, we have:

$x = ((a1 * N1(N1^{-1} \bmod n1) + (a2 * N2(N2^{-1} \bmod n2) +$

$a3 * N3(N3^{-1} \bmod n3)) \bmod N$

$x = (12 * 702 * 13) + (9 * 675 * 25) + (23 * 650 * 14)) \bmod 17550$

$= (109512 + 151875 + 209300) \bmod 17550$

$x = 14387$

(11) For

$a^2 \equiv x \bmod p$, we try values of a from 1 to p-1.

Since we know that $a^2 \bmod p = (p-a)^2 \bmod p$

$\Rightarrow$ there are two different values of a produce the same x.

Hence, the number of quadratic residues modulo p are $\frac{(p-1)}{2}$

Since, the total number of residues are p-1, total number of quadratic non-residues are $(p-1) - \frac{(p-1)}{2} = \frac{(p-1)}{2}$

(12) Since g is generater of Z_p,

$g^{p-1} = 1$

If g is quadratic residue mod p then $g^{\frac{(p-1)}{2}} = 1$

$\Rightarrow$ g can generate only $\frac{(p-1)}{2}$ values which is not true

$\therefore g^{(p-1)/2} \neq 1$

g is quadratic non-residue mod p.

(13) (i) $b^2 \equiv 44 \pmod{83}$

we can write it as : $\begin{bmatrix} 44 \\ 83 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 4 \\ 83 \end{bmatrix} \begin{bmatrix} 4 \\ 83 \end{bmatrix} * \begin{bmatrix} 11 \\ 83 \end{bmatrix}$

$\begin{bmatrix} 83 \\ 4 \end{bmatrix} * \begin{bmatrix} 11 \\ 83 \end{bmatrix}$

$\begin{bmatrix} 3 \\ 4 \end{bmatrix} * \begin{bmatrix} 11 \\ 83 \end{bmatrix}$

$\begin{bmatrix} 3 \\ 2 \end{bmatrix} * \begin{bmatrix} 3 \\ 2 \end{bmatrix} * - \begin{bmatrix} 83 \\ 11 \end{bmatrix}$

$\begin{bmatrix} 1 \\ 2 \end{bmatrix} * \begin{bmatrix} 1 \\ 2 \end{bmatrix} * \begin{bmatrix} 6 \\ 11 \end{bmatrix}$

$1 * \begin{bmatrix} 6 \\ 11 \end{bmatrix} = 0$

ii) $b^2 \equiv 11 \pmod{29}$

we can write it as : $\begin{bmatrix} 11 \\ 29 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 29 \\ 11 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 7 \\ 11 \end{bmatrix}$

$\begin{bmatrix} 7 \\ 11 \end{bmatrix} = 0$

iii) $b^2 \equiv 15 \pmod{59}$

we can write it as : $\begin{bmatrix} 15 \\ 59 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 59 \\ 15 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 14 \\ 15 \end{bmatrix}$

$\begin{bmatrix} 14 \\ 15 \end{bmatrix} = 0$

14) Given $x \equiv y \bmod p$, $x \equiv y \bmod q$

To prove $x \equiv y \bmod N$ $(N = pq)$

Proof:

Chinese Remainder Theorem:

Every pair of congruencies can be uniquely solved for relative prime numbers

Assuming p & q are relatively prime no's $\Rightarrow GCD(p, q) = 1$

$\therefore px + qy = 1$ (for some x, y)

$x \equiv p^{-1} \bmod q$

$y \equiv q^{-1} \bmod p$.

$\therefore p(p^{-1} \bmod q) + q(q^{-1} \bmod p) = 1$

By CRT,

$$x \equiv [y \cdot p(p^{-1} \bmod q) + yq(q^{-1} \bmod p)] \bmod pq$$

$\Rightarrow \because y\,p[p^{-1} \bmod q] + yq(q^{-1} \bmod p) = 1$

$\therefore x \equiv y[1] \bmod pq \equiv y \bmod pq$

$\Rightarrow x \equiv y \bmod N$ $(\because N = pq)$

Hence proved.

15) Assuming p & q are prime numbers

we know that there are $\frac{(p-1)}{2}$ & $\frac{(q-1)}{2}$ possibilities of quadratic residues respectively.

$N = p \times q$

$$x^2 \equiv a \bmod p$$
$$x^2 \equiv a \bmod q$$

then

$$x^2 \equiv a \bmod pq \quad \text{(by CRT)}$$

∴ No. of possibilities of quadratic residues (QR) =

- product of no. of QR's of p & q.

$$= \left(\frac{p-1}{2}\right) \times \left(\frac{q-1}{2}\right).$$

Hence proved.

16) We need to prove that hardness of $x^2 \equiv a \bmod n$.

Proof:

If $A \Rightarrow B$ then $\sim A \Rightarrow \sim B$. i.e.

It's sufficient to prove that easiness of

$x^2 \equiv a \bmod N \Rightarrow$ ease of finding factors of N.

i.e. if factorization is easy

find x in $x^2 \equiv a \bmod N$ is easy.

Let factors of $N = pq$

ii) We can compute x in $x^2 \equiv a \bmod N$ by first computing square root in Z_p of $x \bmod p$. and then in Z_q of $x \bmod q$. Then using CRT we can obtain square root of x in Z_N.

($\because$ $x \bmod pq$ by CRT)

$pq = N$.

So, if n is easy to factorise, then finding x in $x^2 \equiv a \bmod N$ is easy. (~A ⇒ ~B then A ⇒ B)

We can say that it's hard to find x in $x^2 \equiv a \bmod N$ if N is hard to factorize.

Hence proved.

17) We have to prove that if hardness of x in $x^2 \equiv a \bmod N$ ⇒ factors of N.

using if $A \Rightarrow B$, then we can say $\sim A \Rightarrow \sim B$.

factorising is easy ⇒ find x in $x^2 \equiv a \bmod N$. is easy.

We know that $N = pq$

So, we can say that $x^2 \equiv a \bmod N$ is easy if.

$x^2 \equiv a \bmod p \Rightarrow x \equiv a^{\frac{p+1}{4}} \bmod p$.

$x \equiv a^{\frac{p+1}{4}} \bmod q$.

using CRT we can compute x in $x^2 \bmod N$. as p & q are relatively primes. ($N = pq$)

Hence proved.

18) $n = 11 \times 19 = 209$.

$x^2 \equiv 9 \bmod 209$.

$\left(\frac{9}{209}\right) = \left(\frac{2}{9}\right) = 1$.

⇒ By legendre symbol, this equation is solvable.

Here $N = 209$.

$N \bmod 4 = 209 \bmod 4 = 1 \neq 3$.

so $x \equiv 9^{\left(\frac{209-1}{4}\right)} \bmod 209$.

$x \equiv 9^{208/4} \bmod 209$.

$x \equiv 9^{52} \bmod 209$.

$x = 4$.

Another solution $= 209 - 4 = 205$.

Solutions $= 4, 205$ are square roots of $9 \bmod 209$.

19) (1) $\left(\frac{3053}{6823}\right)$.

$\Rightarrow \left(\frac{6823}{3053}\right) \equiv \left(\frac{717}{3053}\right) \equiv \left(\frac{3053}{717}\right) = \left(\frac{185}{717}\right)$

$\equiv \left(\frac{717}{185}\right) = \left(\frac{162}{185}\right) = \left(\frac{2}{185}\right) \times \left(\frac{81}{185}\right)$.

$\equiv \left(\frac{81}{185}\right) = \left(\frac{185}{81}\right) \equiv \left(\frac{23}{81}\right) = \left(\frac{81}{23}\right)$

$\equiv \left(\frac{12}{23}\right) = \left(\frac{2}{23}\right) \times \left(\frac{3}{23}\right) \times \left(\frac{2}{23}\right)$

$\equiv \frac{3}{23} \equiv -\left(\frac{23}{3}\right) = -\frac{2}{3} \equiv -\left(\frac{-1}{3}\right) \times (-1)$

$\equiv 1$.

iii) $\left(\frac{7411}{9283}\right)$.

$= -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right) = -\left(\frac{2}{7411}\right)^4 \times \left(\frac{117}{7411}\right)$.

$= -\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) = -\frac{40}{117} = -\left(\frac{2}{117}\right)^3 \times \left(\frac{5}{117}\right)$

$= \left(\frac{5}{117}\right) = \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right)$.

$= -1$.

20) Sender A sends same message M to 3 people with same $e=3$ and different n.

we can find M in feasable time as follows:

Let's say $n_1 = p_1 q_1$ for first receiver.

$n_2 = p_2 q_2$ (second receiver), $n_3 = p_3 q_3$ (third receiver)

$c_1 = M^3 \% n$ for $e=3$., $c_2 = M^3 \% n$. and.

$c_3 = M^3 \% n$.

Also $M^3 \equiv c_1 \% n_1$, $M^3 \equiv c_2 \% n_2$ and $M^3 \equiv c_3 \% n_3$

with high probability n_1 n_2 and n_3 are relatively prime, so applying CRT.

$M^3 \equiv x \% n_1 n_2 n_3$, $x = M^3 \% n_1 n_2 n_3$, M^3 is hard.

to compute in this case.

$M < n_1$, $M < n_2$, $M < n_3 \Rightarrow M^3 < n_1 n_2 n_3$.

$\Rightarrow M^3 \% n_1 n_2 n_3 = M^3 \Rightarrow M^3 = x \Rightarrow M = x^{1/3}$.

so, this way we can find M.

21 Show that text-RSA is vulnerable under following security notions

(i) IND-CPA (semantic security)

Sol:- Adversary knows his choice of plaintext and corresponding cipher texts.

Chose two mesiages whose jacobi is 1 & -1 as follows :

$m_0 = j[m_0] = 1$

$m_1 = j[m_1] = 1$

Now adversary sends m_0 & m_1 to challenger and he encrypts m_b

$c = e(m_b)$

Now adversary calculates jacobi of m_0 & m_1

if $j[m_b] = 1$ then its m_0

if $j[m_b] = 1$ then its m_1

Hence adversary correctly guessed. Therefore it is not semantically secure under IND-CPA

ii) IND-CCA

Sol:- $c^* = (m^e) \bmod n$ c_1, c_2 adversary chose -x.

$c_1 = x^e \bmod n$ - can be known since e is public

$c_1 = (m^*)^e \bmod n$

$c, c^* = (x m^*)^e \bmod n$

he will ask what is plaintext for c, c^*.

So plaintext becomes $x m^*$, $m^* = x m^* x^{-1} \bmod n$

22. If m is chosen from a small list of possible values ($m < 2^l$, m has l-bits). Show that attacker can compute message m in time $O(l 2^{\alpha l})$, $1/2 < \alpha < 1$ which is better than brute force method. (Meet in middle attack)

Sol:-

Meet in the middle attack

Let $c = m^e$

Assume $m = rs$

Therefore $c = (rs)^e$

$c/(r)^e = s^e$

Let m be 'l' bits long. For all $r < 2^{l/2}$ find $c/(r)^e$ & store the values in sorted order in a table.

Now pick a random s and compute s^e and check if this value exists in the table. If it exists, then we know r & s, so we can compute $m = rs$. If it does not exist then pick another s.

Time for generating and computing c/re all possible values of $r = O(2^{\ell/2})$.

Time for sorting $= O(2^{\ell/2} \log(2^{\ell/2}))$

Time for searching all possible values of $s = 2^{\ell/2} O(\log(2^{\ell/2}))$

Therefore total time $= O(2^a)$ when $\ell/2 < a < \ell$

23. Let (Gen, E, D) be a chosen ciphertext secure public-key encryption system with message space $\{0,1\}^{128}$. Which of the following is also chosen ciphertext secure.?

(i) (Gen, E', D') where $E'(pk, m) = E(pk, m \oplus 1^{128})$ & $D'(sk, c) = D(sk, c) \oplus 1^{128}$

Sol:- This scheme is chosen ciphertext secure, since the only thing extra in this scheme is inverting the message before encryption. The original scheme is chosen ciphertext secure so this scheme also is chosen ciphertext secure

ii) (Gen, E', D') where $E'(pk, m) = (E(pk, m), E(pk, 0^{128}))$ and $D'(sk, (c_1, c_2)) = D(sk, c_1)$.

Sol:- This scheme is not chosen ciphertext secure. The attacker can send any two messages m_0 & m_1. The challenger will then send the ciphertext (c_1, c_2). The attacker can then ask for the decryption of $(c_1, E(1^{128}))$ for

which the challenger will either send m_0 or m_1. Using that the attacker can identify which of m_0 or m_1 was encrypted.

iii) $(Kgen, E', D')$ where $E'(pk, m) = (E(pk, m), E(pk, m))$ and

$$D'(sk, (c_1, c_2)) = D(sk, c_1).$$

This scheme is not chosen ciphertext secure. The attacker can send any two messages $m_0 \& m_1$. The challenger will then send the ciphertext (c_1, c_2). The attacker can then ask for the decryption of $(c_1, E(m_2))$, where m_2 is some random message (high probability that $E(m_2)$ is not $E(m_0)$ or $E(m_1)$, for which the challenger will either send m_0 or m_1. Using that the attacker can identify which of m_0 or m_1 was encrypted.

24)

Bob's experiment:

Input : $f(x)$

Output : parity of $f(x)$

Algorithm : If $[f(x)]_0 = 0$, then x is even, else x is odd.

Bobs probability of success :-

If x is chosen of random,

$Pr[x \text{ is even}] = Pr[x \text{ is odd}] = 1/2$

$Pr[\text{Bob succeeds}] = Pr[x \text{ is even}] * Pr[\text{Bob succeeds} \mid x \text{ is even}]$

$+ Pr[x \text{ is odd}] * Pr[\text{Bob succeeds} \mid x \text{ is odd}] =$

$$1/2 \times \frac{1}{2} + \frac{1}{2} \times 1$$

$$= 3/4$$

Alices's cheating probability :-

We compute Alice's cheating probability irrespective of Bob's strategy.

Alice can cheat by changing the Parity of x.

case 1 : x is even.

$f(x)]_0 = 0$, with probability $= 1/2$.

In this case Alice cannot cheat.

$f(x)]_1 = 1$, with probability $= 1/2$.

In this case Alice can cheat.

So, in this case, probability of sucess for Alie $= 1/4$

case 2: x is odd.

$f(x)]_0 = 0$, This is not possible from the definition of f.

$f(x)]_0 = 1$, In this case Alice can cheat, So In this case probability of ~~success~~ for Alice $= 1/2$.

So, Alice can cheat with probability of $1/4 + 1/2 = 3/4$.

$\times$