S20180010017
ASHUTOSH CHAUHAN

Cryptography

Q.1)

(a). (i) Confidentiality → Since the message is encrypted using a secure encryption algorithm i.e. the message is confidential.

(ii)

(b) $a = 10$, $b = 26$.

$\gcd(a, b) \Rightarrow 2$

find x, y such that $ax + by = 2 \rightarrow 10x + 26y = 2$

finding gcd →

$26 = 2 \times 10 + 6$ — ①

$10 = 1 \times 6 + 4$ — ②

$6 = 1 \times 4 + 2$ — ③

$4 = 2 \times 2 + 0$ — ④

gcd

$6 \Rightarrow 26 - 2 \times 10$

$4 \Rightarrow 10 - 1 \times (26 - 2 \times 10)$

$4 \Rightarrow 10 - 26 + 10 \times 2 \rightarrow 10 \times 3 - 26$

$2 \rightarrow 6 - 4$

$\rightarrow 26 - 2 \times 10 - (10 \times 3 - 26 + 10 \times 3)$

$\rightarrow 26 - 2 \times 10 + 26 - 10 \times 3$

$2 \rightarrow 26 \times 2 - 5 \times 10$

$a = -5$
$b = 2$ Ans.

S2018 001 0017
Ashutosh Chauhan

Q 1.

(c) In a cryptosystem $(P, K, C, \mathcal{E}, D)$

let there be x_1, x_2 s.t. $x_1 \neq x_2$ and.

such that $x_1 = D_K(y)$ — ①

$x_2 = D_K(y)$ — ②

now lets have

$y_1 \Rightarrow \mathcal{E}_K(x_1)$ and

$y_2 \Rightarrow \mathcal{E}_K(x_2)$

due to the nature of function $\mathcal{E}$ $y_1 \neq y_2$ (encrypt function) which contradicts our assumption according to ① and ②

hence our assumption is wrong and $x_1 = x_2$.

Hence Proved for a cyphertext y, key k there exists only one x such that $x = D_K(y)$.

Q. 2.) $P \rightarrow \{a, b, c, d\}$
$K \rightarrow \{k_1, k_2, k_3, k_4\}$
$C = \{1, 2, 3, 4, 5\}$

$P_r[a] = 1/6$		$P_r[k_1] \rightarrow 1/4$
b	1/3	$k_2 \rightarrow 1/2$
c	1/3	$k_3 \rightarrow$
d	1/2	$k_4 \rightarrow 1/8$
		1/8

	a	b	c	d
k_1	1	2	3	4
k_2	2	1	5	3
k_3	4	2	1	5
k_4	3	1	5	2

$Pr[1] \Rightarrow \sum P_r[K = k] \cdot P_x[x = D_k(1)]$

$\Rightarrow \frac{1}{4} \times \frac{1}{6} + \frac{1}{2} \times \frac{1}{3} + \frac{1}{8} \times \frac{1}{3} + \frac{1}{8} \times \frac{1}{3}$

$\rightarrow \frac{7}{24}$

$Pr[2] \Rightarrow Pr$ for $(k_1, b) \ldots (k_4, d)$

$\rightarrow \frac{1}{4} \cdot \frac{1}{3} + \frac{1}{2} \cdot \frac{1}{6} + \frac{1}{8} \cdot \frac{1}{3} + \frac{1}{8} \cdot \frac{1}{6} \Rightarrow \frac{4+2+1}{48} \rightarrow \frac{11}{48}$

Q. 2

S20180010017
ASHUTOSH [illegible]

$P_r[3]$

$\frac{1}{4} + \frac{1}{3} + \frac{1}{2} \times \frac{1}{6} + \frac{1}{8} \cdot \frac{1}{6} \rightarrow \frac{3}{16}$

$P_r[4] \rightarrow \frac{1}{4} \times \frac{1}{6} + \frac{1}{8} \times \frac{1}{6} \rightarrow \frac{1}{16}$

$P_r[5] \rightarrow \frac{1}{2} \times \frac{1}{3} + \frac{1}{8} \cdot \frac{1}{6} + \frac{1}{8} \cdot \frac{1}{3} = \frac{8+1+2}{48} \rightarrow \frac{11}{48}$

Non-uniform distribution

(ii) $H(r) \rightarrow -\sum_{x \in X} P_r[x] \log_2 P_r[x]$

$-\left[\frac{7}{24} \log 7/24 + \frac{11}{48} \log \frac{11}{48} + \frac{3}{16} \log \frac{3}{16} + \frac{1}{16} \log \frac{1}{16} + \frac{11}{48} \log \frac{11}{48}\right]$

$\Rightarrow \underline{2.195}$ Ans

S20180010017
ASHUTOSH CHAUHAN

Q.3]

Given P[10] → 3 5 2 7 4 | 10 1 9 8 6

P8 → 6 3 7 4 8 5 10 9

IP → 2 6 3 1 4 8 5 7

IP⁻¹ → 4 1 3 5 7 2 8 6

E/P → 4 1 2 3 2 3 4 1

P4 → 2 4 3 1

a) p = 11, q = 31, s = 5

n = 11 × 31 → 341

$x_0 = s^2 \% n \rightarrow 25$

$x_1 \rightarrow 25^2 \% n \rightarrow 284$

$x_2 \rightarrow 284^2 \% n \rightarrow 180$

$x_3 \rightarrow 180^2 \% n \rightarrow 5$

$x_4 \rightarrow 5^2 \% n \rightarrow 25$

$x_5 \rightarrow 25^2 \% n \rightarrow 284$

$x_6 \rightarrow 284^2 \% n \rightarrow 180$

$x_7 \rightarrow 180^2 \% n \rightarrow 5$

$x_8 \rightarrow 5^2 \% n \rightarrow 25$

$x_9 \rightarrow 25^2 \% n \rightarrow 284$

$x_{10} \rightarrow 284^2 \% n \rightarrow 180$

$x_i \% 2$
0
0
1
1
0
0
1
1
0
0

pseudorandom key(K) → 1 2 3 4 5 6 7 8 9 10 : 0 0 1 1 0 0 1 1 0 0

(b) $K_1 \rightarrow P8(SF_1(P10(K)))$, $K_2 \rightarrow P8(SF_2(SF_1(P10(K))))$

→ P10(K) → 1 0 0 1 1 | 0 0 0 1 0

$SF_1(P10(K))$ → 0 0 1 1 1 | 0 0 1 0 0

$K_1 = P8(SF_1(P10(K)))$ → 0 1 0 1 1 1 0 0

$SF_2(P10(K))$ → 1 1 1 0 0 | 1 0 0 0 0

$K_2 \rightarrow P8(SF_2(SF_1(P10(K))))$ → 1 1 0 0 0 0 0 0