IT 352 :- Information Assurance & Security

Assignment 2

Chinmayi C. Ramakrishna
181IT113

5th Feb, 2021

Step 1 :- Choose p and q, p = 3, q = 11

Step 2 :- $n = p \times q = 3 \times 11 = 33$

Step 3 :- $A = (p-1)(q-1) = 2 \times 10 = 20$

Step 4 :- E = 7, $1 < E < A$, $\gcd(E, A) = 1$

Step 5 :- D = 3 $DE - 1$ = multiple of A, $1 < D < A$.

Message encryption

E	K	C
↓	↓	↓
3	4	5
↓	↓	
2187	16384	78125
↓	↓	↓
9	16	14

Raise to E = 7.

Divide by n = 33

Encrypted message = 9 16 14

Message decryption

9	16	14	
↓	↓	↓	
729	4096	2744	Raise to D = 3
↓	↓	↓	
3	4	5	Divide by n = 33
↓	↓	↓	
E	K	C	

Decrypted message = E K C

Step 1 :- Choose p and q, $p = 17$, $q = 29$

Step 2 :- $n = p \times q = 17 \times 29 = 493$

Step 3 :- $A = (p-1)(q-1) = 16 \times 28 = 448$

Step 4 :- $E = 5$, $1 < E < A$, $\gcd(E, A) = 1$

Step 5 :- $D = 269$, $1 < D < A$, $DE - 1 =$ multiple of A

Message encryption

C	H	
↓	↓	
4	6	Numbers assigned
↓	↓	
1024	7776	Raise to $E = 5$
↓	↓	
38	381	Divide by $n = 493$ and find remainder

Encrypted message = 38 381

Message decryption

38	381	
↓	↓	
38^{269}	381^{269}	Raise to $D = 269$
↓	↓	
4	6	Divide by $n = 493$
↓	↓	
C	H	

Decrypted message = CH