**Multiplicative Ciphers**

**Affine Cipher**

**Key 1 = a; Key 2 = b.**

**X = C A R (2, 0, 17)**

**a = 5; b = 8;**

**Encryption**

**Y = (aX + b) Mod 26**

**= (5\*2 + 8) Mod 26 = 18 Mod 26 = 18 🡪 S**

**= (5\*0 + 8) Mod 26 = 8 mod 26 = 8 🡪 I**

**= (5\*17 + 8) Mod 26 = 93 Mod 26 = 15 🡪 P**

**Y = S I P (18, 8, 15)**

**Decryption**

**X = (Y – b).a-1 Mod 26**

**5-1 Mod 26**

**X = (Y – b). 5-1 Mod 26**

**X = (Y – b). 21 Mod 26**

**Multiplicative inverse ?**

**p . q mod 26 = 1**

**p . q = 1 mod 26**

**p . 5 = 1 mod 26**

**1 Mod 26 = 1**

**27 Mod 26 = 1**

**53 mod 26 = 1**

**79 mod 26 = 1**

**105 Mod 26 = 1 => 105 / 5 = 21**

**131 Mod 26 = 1**

**157 Mod 26 = 1**

**.**

**p . q = 1 mod 26**

**21 . 5 = 1 mod 26**

**a-1 =21**

**Decryption**

**Y = S I P (18, 8, 15)**

**X = (Y – b).a-1 Mod 26**

**= (18 – 8) . 21 Mod 26 = 210 Mod 26 = 2 🡪 C**

**= ( 8 – 8) . 21 Mod 26 = 0 Mod 26 = 0 🡪 A**

**= (15 – 8) . 21 Mod 26 = 147 Mod 26 = 17 🡪 R**

**We can’t calculate multiplicative inverse of every number**

**Number (a) have to be co-prime with the domain (n)**

**2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24,**

**We cannot calculate 13-1 when domain is 26 (13 and 26 are not co-prime)**

**We cannot calculate 5-1 when domain is 25 (5 and 25 are not co-prime)**

**(5, 26) inverse of 5 is possible in domain of 26**

**(5,25) it is not possible 5 and 25 are not co-prime**

**GCD (13, 26) = 13 inverse is not possible**

**Crypt-Analysis of Affine Cipher**

**X = C A R (2, 0 , 17)**

**Y = S I P (18, 8, 15)**

**Plain-cipher text pair (2 characters)**

**Y = (aX + b) Mod 26**

**C 🡪 S**

**A 🡪 I**

**R 🡪 P**

**18 = (2a + b) Mod 26**

**8 = (0a + b) Mod 26**

**8 = b mod 26**

**b = 8**

**18 = 2a + 8 Mod 26**

**18-8 = 2a Mod 26**

**10 = 2a Mod 26**

**2a = 10**

**a = 5**

**15 = (17a + b) Mod 26**

**18 = (2a + b) Mod 26**

**a = ?**

**b =?**

**HILL CIPHER**

**(Matrix Multiplication)**

**X = P A Y (15 0 24)**

**X =**

**KX = XK ?matrix multiplication?**

**Y = KX MOD 26**

**No of col. of first matrix = no. of rows of second matrix**

**Y = K . X mod 26**

**. Mod 26**

**Y = K . X mod 26**

**. Mod 26**

**X = K-1 . Y mod 26**

**A-1 =**

**|K| = 17 (18\*19 – 2\*21) - 17(21\*19 – 2\*21) + 5(21\*2 – 2\*18)**

**= 17 (342 – 42) – 17(399 – 42) + 5(42-36)**

**= -939**

**c11 = (-1) 1+1 (18\*19 – 2\* 21) = 300**

**c12 = (-1) 1+2 (21 \* 19 – 2\*21) = -357**

**c13 = (-1) 1+3 (21\*2 – 2\*18) = 6**

**c21 = (-1) 2+1 (17\*19 – 2\*5) = -313**

**c22 = (-1) 2+2 (17\*19 – 2\*5) = 313**

**c23 = (-1) 2+3 (17\*2 – 2\*17) = 0**

**c31 = (-1) 3+1 (17\*21 – 18\*5) = 267**

**c32 = (-1) 3+2 (17\*21 – 21\*5) = -252**

**c33 = (-1) 3+3 (17\*18 – 21\*17) = -51**

**=> transpose =>**

**K-1 =**

**K-1 =**

**X = K-1Y mod 26**

**= mod 26**

**-939 + 37\*26 = 23**

**= mod 26**

**= mod 26**

**Multiplicative inverse of 23 is 17**

**mod 26**

**We can not calculate 13-1 when domain is 26 (13 and 26 are not co-prime)**

**Hill Cipher**

**Encryption**

**X = P A Y (15 0 24)**

**K [3x3]**

**K =**

**X =**

Y = KX mod 26

Y =  **. Mod 26**

**Y =**  Mod 26

Y =

**Y =**