Useful substitutions

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Exercise *Encrypt the plaintext string THE WEATHER IS BAD, by using the the shift cipher with key* $k = 11$.

Exercise *By using the Caeser cipher encrypt the message STOP TALKING IN THE CLASS.*

Exercise *The following ciphertext string has been obtained by using the shift cipher with key* $k = 7$: *HYTF PZ JXTPUN. Find the plaintext string.*

Exercise *Which of the following ordered pairs of numbers are the keys for the affine cipher.* $(2, 9)$, $(3, 11)$, $(17, 17)$, $(7, 0)$, $(13, 2)$ *modulo 26?*

Exercise *Find the inverses of the following: 2 modulo 9, 11 modulo 45, 35 modulo 64, 21 modulo 29, 10 modulo 13.*

Exercise *For which of the following the inverses exist ? 19 modulo 26, 10 modulo 66, 71 modulo 99, 12 modulo 84.*

Exercise *An encrytion rule* e_K *for the affine cipher is given by the formula,* $e_K(x) = 5x + 1$. *Find the key K and the decryption rule* d_K. *Find all those letters that are invariant under* e_K.. *A decryption rule* d_K *for the affine cipher is given by the formula* $d_K(y) = 9y + 20$, *find the key K and the encryption rule* e_K. *Use this key to encrypt THE IDEA IS WONDERFUL. Find all those letters that remain invariant under* e_K

Exercise *Encrypt the plain text string A TOWERING PERSONALITY WINS, by using the following.*

(a) *The affine cipher with key* $(3, 7)$.

(b) *The affine cipher with decryption rule* $d_K(y) = 15y + 20$.

(c) *The permutation cipher with key* $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

(d) *The Vigenere cipher with key* $k = (4\ 6\ 9\ 3)$.

Exercise *The following ciphertext string has been obtained by using the shift cipher, UCGO QMRH MW IZMP. Find a key such that by using it you get a sensible plaintext string. Find such a plaintext string.*

Exercise *If the encryption rule* e_K *for an affine cipher is such that* $e_K(B) = N$ *and* $e_K(E) = S$. *Find the encryption rule. Use this encryption rule to find the ciphertext string for the plaintext string KING SAUD UNIVERSITY.*

Exercise *Find the number of keys for the following affine ciphers.*

(a) *modulo 26,*
(b) *modulo 30,*
(c) *modulo 81,*
(d) *modulo 97.*

Exercise *The message WEZBFTBBNJ THNBT ADZQE TGTYR BZAJN ANOOZATWGNABOVG FNWZV A was enciphered by using an affine cipher transformation. If you know that the most common letters in the plain text are A, E, N and S, find the plaintext message.*

Exercise *If* $m = p^2 q$, *where p, q are two distinct prime numbers, find the number of keys in the affine cipher modulo m.*

Exercise *Find all the non-singular* 2×2*-matrices modulo 2.*

Exercise *Find the number of non-singular matrices, in each of the following cases.*

(a) 3×3*-matrices modulo 54.*
(b) 4×4*-matrices modulo 26.*
(c) 5×5*-matrices modulo 72.*
(d) 2×2*-matrices modulo 3 having deteminant one.*

Exercise *Consider the permutations*

$$\pi = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ z & y & x & w & v & u & t & s & r & q & o & n & m & l & p & k & j & i & h & g & f & e & d & c & b & a \end{pmatrix}$$

$$\eta = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & c & d & e & a & j & h & i & g & k & l & m & o & p & q & r & s & t & n & f & z & y & x & w & v & u \end{pmatrix}.$$

(a) Find $\pi^{-1}, \eta^{-1}, \pi^2, \pi\eta, \eta\pi, \eta^{-1}\pi^{-1}$.
(b) Consider the plaintext string FRIDAYS ARE HOLIDAYS. Find its ciphertext strings by using each of the following encryption rules in the substitution cipher: e_π , $e_{\pi^{-1}}$, $e_{\pi^{-1}\eta}$, e_{η^3}.
(c) Consider the ciphertext string HAZLUTJKL YGZ CZMM WRJLZK. It has been obtained by applying one the following keys : $\pi, \eta, \pi\eta, \eta^2$ in the substitution cipher. Find the key by applying which you get a meaningful plaintext string.

Exercise *Consider a cryposystem ($\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$) with $\mathcal{P} = \mathcal{C}$. For any key $K \in \mathcal{K}$, prove that the encryption rule e_K and the decryption rule d_K both are one-to-one and onto functions. If for some keys $K, K' \in \mathcal{K}$ the composite function $e_K \circ e_{K'} = e_L$ for some $L \in \mathcal{K}$, then the key L is called the* ***product*** *KK' of the keys K and K'. Prove the following.*

(a) *Consider the affine cipher ($\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$) with $\mathcal{P} = \mathcal{C} = Z_m$ for some positive integer m. For any two keys K, K' in $\mathcal{K}$ prove that there exists product $KK' \in \mathcal{K}$. Prove that this composition makes $\mathcal{K}$ a group. Find a subgroup of $\mathcal{K}$ of order m.*
(b) *Let ($\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$) be the substition cipher. Prove that $\mathcal{K}$ is a group of order 26! under the operation of finding products of keys.*

Exercise *Find determinant of each of the following matrix. Which of these matrices are non-singular ? Find inverse of each of that matrix which is non-singular.*

(a) $\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}$ *modulo 10.*

(b) $\begin{bmatrix} 5 & 2 \\ 6 & 7 \end{bmatrix}$ *modulo 25.*

(c) $\begin{bmatrix} 4 & 2 & 0 \\ 0 & 1 & 3 \\ 1 & 3 & 4 \end{bmatrix}$ *modulo 13,*

(d) $\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ *modulo 26.*

(e) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 2 & 4 \end{bmatrix}^2$ *modulo 13.*

Exercise *Encrypt the plaintext string WAR STARTED by using the key* $K = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$ *in the Hill cipher. Find the decryption rule (decrypting key)* d_K*. Use it to decrypt the ciphertext string VEDUKQXLJGTF. Find all the digraphs* P_1P_2 *that remain invariant under* e_K*.*

Exercise *Encrypt the plaintext string HARD WORK ALWAYS HELPS US by using each of the following keys.*

(a) $K = \begin{bmatrix} 3 & 0 & 1 \\ 0 & 0 & 1 \\ 3 & 1 & 0 \end{bmatrix}$ *in the Hill cipher*

(b) $K = (4, 2, 0, 3)$ *in the Vinegere cipher.*

(c) *Permutation* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 6 & 7 & 5 & 2 & 1 \end{pmatrix}$ *in a permutation cipher of length 7.*

Exercise *For* $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$ *find* $B^{-1}A$ *over* Z_{26}*. Use the key* $K = B^{-1}A$ *in the Hill cipher to encrypt the plaintext string MONEY DOES NOT HELP.*

Exercise *Find, if possible, the key K in the Hill cipher with length* $m = 2$ *that gives the ciphertext string UPDL from the plaintext string GO ON.*

Exercise *Does there exists a keys K of length m in the Hill cipher in the following cases ?*

(a) $m = 2$, *that transforms the plaintext string GO ON to the ciphertext string UN LB.*

(b) $m = 2$, *that transforms the plaintext string GO ON to the ciphertext string SS QN.*

Exercise *Find the key K of length* $m = 3$ *in the Hill cipher that gives the ciphertext string OJQR XCOKT from the plaintext string OVER GROWN. Find* K^{-1}*. Use the encrypting key* d_K *to decrypt the ciphertext string.*

EAEBOWLRNOWL.

Exercise *Show that the product cipher obtained by enciphering with a Hill cipher of length m followed by using a Hill cipher of length n, is Hill cipher of length* $l.c.m(m, n)$.

Exercise *If you know that a permutation cipher with length* $m = 5$ *was used to obtain the ciphertext string LAYLA COAIS NNOMM INEAM BIAAR NGACL EXGUA, find the plaintext string.*

Exercise *Define a stream cipher? Explain how a Vinegere cipher of length m can be thought of as a synchronous stream cipher of periodicty m.*

Exercise *Consider the stream cipher* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$ *with* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = Z_{26}$ *and* $\mathcal{F}$ *the key stream generator consisting of the functions* f_i *with* $z_1 = f_1(k_1) = k_1$, *for* $i \geqslant 2$, $z_i = f(k_1, x_1, x_2, \ldots, x_{i-1}) = k_1 + x_1 + x_2 + \ldots + x_{i-1}$. *Further, for any* $z \in \mathcal{L}$ *the encryption rule is given by* $e_z(x) = x + z \bmod 26$. *Answer the following.*

(a) *For the seed* $k = 5$, *and the plain text TODAY IS A PICNIC DAY, generate the key stream.*

(b) *Encipher the plaintext string WAR IS LOOMING ON THE HORIZON by using seed* $k = 3$.

(c) *The ciphertext string IWKNOMQIQH has been obtained by using the seed* $k = 2$. *Decipher it.*

(d) *Is this stream cipher synchronous?*

(e) *If the ciphertext string written in numerals is* $y_1 y_2 y_3 y_4 y_5 y_6$ *and it is known that the seed is* $k = 6$, *find the plaintext string and the key stream.*

Exercise *Consider the stream cipher with* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = Z_{26}$. *Further, the key stream generator* $\mathcal{F}$ *consists of the functions* f_i *given as follows.* $f_1(k_1) = k_1$, *and for* $i \geqslant 2$, $f_i(k_1, x_1, x_2, \ldots, x_{i-1}) = ik_1 \bmod 26$. *For any* $z \in \mathcal{L}$, *the encryption rule is given by* $e_z(x) = x + z \bmod 26$.

(a) *Prove that this cipher is synchronous and periodic.*

(b) *By using the seed* $k = 9$, *encrypt the plaintext string THIS CIPHER IS SURELY USEFUL.*

Exercise *Solve the system of congruences*

$$\begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{9} \end{aligned}$$

Exercise *Solve the following system of congruences.*

$$\begin{aligned} x &\equiv 2 \pmod{6} \\ x &\equiv 0 \pmod{5} \\ x &\equiv -3 \pmod{7} \end{aligned}$$

Exercise *Solve the system of congruences*

$$\begin{aligned} x &\equiv 5 \pmod{2} \\ x &\equiv -5 \pmod{11} \\ x &\equiv 13 \pmod{7} \end{aligned}$$

Exercise *Find* $x \in Z_{2002}$ *satisfying the following system of congruences :*

$$\begin{aligned} x &\equiv 10 \pmod{14} \\ x &\equiv 9 \pmod{11} \\ x &\equiv 12 \pmod{13} \end{aligned}$$

Exercise *Show that the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

where m_1, m_2 are positive integers, has a solution iff $gcd(m_1, m_2) \mid (a_1 - a_2)$.

Exercise *Find the general solution of the system of congruences*

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 7 \pmod{6} \end{aligned}$$

Find if possible, its solution in Z_{12}.

Exercise *Find primitive elements in each of the following:* $Z_{13}^*, Z_{17}^*, Z_{29}^*$.

Exercise *Let A and B be two* $n \times n$ *matrices over a field F. Prove that there exists a non-singular* $n \times n$ *matirx K such that* $AK = B$ *iff A and B have same column spaces iff* A^T *and* B^T *are row equivalent iff* A^T *and* B^T *can be reduced to same matrix in reduced row echelon* *form.*

Exercise *Find the (minimum) number of binary digits one needs for each of the following integers for their expression in binary digits. 49, 77, 100, 175, 2505.*

Exercise *Write each of the following integers in binary digits 31, 29, 50. By using square and multiply rule find the following:* $15^{31} \pmod{41}$, $17^{29} \pmod{23}$, $4^{50} \pmod{25}$.

Exercise *Find all the keys* $K = (a, n)$ *in the RSA-public key cryposystem given by* $n = 77$. *Given the key (7, 77) encipher the plaintext message CHEER UP.*

Exercise *Given n and* $\Phi(n)$ *find prime numbers p, q such that* $n = pq$ *in each of the following cases.*

(a) $n = 291, \Phi(n) = 192$.

(b) $n = 7663, \Phi(n) = 7488$.

(c) $n = 1381, \Phi(n) = 1264$.

In each case find the number of pairs (a, b) of elements of $Z_{\Phi(n)}$ such that $ab \equiv 1(\mathrm{mod}\,\Phi(n))$.

Exercise *Consider the modulus exponentiation cipher with modulus prime* $p = 29$

(a) *Encipher the plaintext string LOTS HAVE NOTHING by using key* $k = 7$.

(b) *Decipher the cipher string 23 03 27 10 05 12 by using the key* $k = 11$.

(c) *Find all the keys.*

(d) *Find all those keys k for which the encryption rule and the decryption rules ars the same.*

(e) *If the base number is* $r = 5$, *two individuals have keys* $k_1 = 9$, $k_2 = 11$ *respectively, find the common key.*

Exercise *Find the largest length m of the block of letters of a plaintext string for the modulus exponentiation cipher, if modulus primes p are given as (i)* $p = 29$, *(ii)* $p = 101$, *(iii)* $p = 1019$, *(iv)* $p = 2459$ *(v)* $p = 3779$. *For each of these exponential ciphers find the number of keys.*

Exercise *Consider the modulus exponentiation cipher with modulus prime* $p = 2591$. *Decrypt the ciphertext string*

2093 1372 0460 1797.

Exercise *Consider the modulus exponentiation cipher with modulus prime* $p = 101$ *with base* $a = 7$. *If two individuals have respective keys* $k_1 = 27$ *and* $k_2 = 31$, *find their common key k.*

Exercise *List all pairs of primes* (p, q) *with* $q < p < 200$ *and* $p = 2q + 1$.

Exercise *For* $n = 2881$, *find* $\Phi(2881)$. *If the ciphertext message produced by the RSA cipher with key* $(a, n) = (5, 2881)$ *is 0504 1874 0347 0515 2088 2356 0736 0468, what is the plain text message.*

Exercise *Consider an RSA cipher with modulus* $n = 53 \cdot 71$.

(a) *Suppose a member A of the RSA cipher has selected the key* $(11, 53 \cdot 71)$. *If B sends him the message NOW, what is the ciphertext message received by A.*

(b) *Find the deciphering key for A. If A has received the ciphertext message 0737 1627, find the plaintext message that was sent to A.*

Exercise *In an RSA cipher with modulus n, suppose an opponent finds a plaintext whose numerical equivalent in not relatively prime to n. Explain how can he use this fact to brake the cipher.*

Exercise *Harold and Audrey have as their RSA keys (3, 23.47) and (7, 47.59) respectively.*

(a) *What is the signed ciphertext message sent by Harold to Audrey, when the plaintext message is WELCOME AUDREY.*

(b) *What is the signed ciphertext message sent by Audrey to Harold, when the plaintext message is THANK YOU.*

Exercise *If in an RSA cipher the enciphering key* (e, n) *is so chosen that* $2^e > n$*, if a ciphertext* $C \neq 1$ *is intercepted, explain why the intercepter cannot get the plaintext block P by simply finding the* $e-th$ *root of C.*

Exercise *Let* $n = pq$ *where p, q are two distinct odd primes. Let* $m = l.c.m(p-1, q-1)$.

(a) *Is* $m = \Phi(n)$?

(b) *Can you design a public key system similar to PSA system by using m instead of* $\Phi(n)$*? Explain.*

Exercise *For each of the following recurrence relations answer the following.*

(a) $z_{i+3} = z_{i+1} + z_i$.

(b) *For the initial values* $z_0 = 0, z_1 = 1, z_2 = 1$*, generate the sequence* $\{z_i\}$ *and find its periodicity. Use it to encipher the plaintext message GOOD MORNING*

(c) *Do same thing if the initial values are* $z_0 = 1, z_1 = 0, z_2 = 1$.

(d) *Show that the characteristic polynomial* $x^3 + x + 1$ *is irreducible over* Z_2.

(e) $z_{i+4} = z_{i+3} + z_i$*. Generate the sequence* $\{z_i\}$ *with initial values* $z_0 = 0, z_1 = 0, z_2 = 0, z_3 = 1$*. Check that its period is 15.*

(f) *)* $z_{i+5} = z_{i+1} + z_i$*. By choosing any set of initial values generate a sequenc and verify that its period is a factor of 21.*

Exercise *Compute each of the following Jacobi symbol.* $(\frac{2}{115}), (\frac{400}{975}), (\frac{39}{49}), (\frac{39}{13})$.

Exercise *Solve* $x^2 \equiv 1(mod 253)$.

Exercise *Solvex*$^2 \equiv 1(mod 291)$.

Given a positive integers b, a positive integer n is called a **pseudo prime** to base b, if $b^n \equiv b(\bmod n)$

Exercise *Show that 91 is a pseudo prime to base 3.*

Exercise *Show that 368 is a pseudo prime to bases 17 and 19.*

Exercise *Let* $n = 391, a = 15, b = 47$ *be such that* $ab \equiv 1(mod\Phi(n))$*. We are not supposed to know* $\Phi(n)$*. By using Las Vegas test and by using number* $\omega = 5$*, see if you can find two prime numbers p, q such that* $n = pq$.