Sara Baradaran
9624193

1.7

1. The addition and multiplication table for Z_4

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2. The addition and multiplication table for Z_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

3. The addition and multiplication table for Z_6

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

4. For all elements like q which $q \in Z_x$ & $\gcd(x, q) \neq 1$ → a multiplicative inverse doesn't exist for q

$Z_4 = \{0,1,2,3\}$ q = 0,2

$Z_6 = \{0,1,2,3,4,5\}$ q = 0,2,3,4

5 is a prime number so there is no element like $q \neq 0$ in Z_5 which $\gcd(5, q) \neq 1$ (for all elements like $q \neq 0$ which $q \in Z_5$ → $\gcd(q, 5) = 1$) so a multiplicative inverse exist for all nonzero elements in Z_5.

1.5

1. $15 * 29 \equiv 15 * 29 \equiv 2 * 3 \equiv 6 \pmod{13}$

2. $2 * 29 \equiv 2 * 29 \equiv 2 * 3 \equiv 6 \pmod{13}$

3. $2 * 3 \equiv 2 * 3 \equiv 2 * 3 \equiv 6 \pmod{13}$

4. $-11 * 3 \equiv -11 * 3 \equiv 2 * 3 \equiv 6 \pmod{13}$

Result → $15 * 29 \equiv 2 * 29 \equiv 2 * 3 \equiv -11 * 3 \pmod{13}$

1.8

multiplicative inverse of a = 5 in Z_{11} , Z_{12} , Z_{13} :

$\varphi(11) = 10 \rightarrow a^{-1} \equiv 5^{10-1} \equiv 9 \pmod{11}$

$\varphi(12) = 4 \rightarrow a^{-1} \equiv 5^{4-1} \equiv 5 \pmod{12}$

$\varphi(13) = 12 \rightarrow a^{-1} \equiv 5^{12-1} \equiv 8 \pmod{13}$

1.9

$X = 3^2 = 9 \pmod{13} \rightarrow X = 9$

$X = 7^2 \equiv 10 \pmod{13} \rightarrow X = 10$

$X = 3^{10} = 3^3 * 3^3 * 3^3 * 3 \equiv 1 * 1 * 1 * 3 \pmod{13} = 3 \rightarrow X = 3$

$X = 7^{100} \equiv (7^2)^{50} \equiv 10^{50} \equiv (10^2)^{25} \equiv 9^{25} \equiv (9^2)^{12} * 9 \equiv 3^{12} * 9 \equiv (3^4)^3 * 9 \equiv 3^3 * 9 \equiv 1 * 9 \equiv 9 \pmod{13}$ → $X = 9$

$7^x = 11 \bmod 13 \rightarrow 13 * q + 11 = 7^x \ (q \in Z) \rightarrow X = 5$

1.10

$\varphi(4) = 4 * (1-\frac{1}{2}) = 2 \rightarrow \{1,3\}$

$\varphi(5) = 5 - 1 = 4 \rightarrow \{1,2,3,4\}$

$\varphi(9) = 9 * (1-\frac{1}{3}) = 6 \rightarrow \{1,2,4,5,7,8\}$

$\varphi(26) = 26 * (1-\frac{1}{13}) * (1-\frac{1}{2}) = 12 \rightarrow \{1,3,5,7,9,11,15,17,19,21,23,25\}$

1.13

$Y_1 = ax_1 + b \bmod 26$

$Y_2 = ax_2 + b \bmod 26$ → $y_1 - y_2 = a\,(x_1 - x_2) \bmod 26 \rightarrow a = \frac{y1-y2}{x1-x2} \bmod 26$

→ $y_2x_1 - y_1x_2 = b\,(x_1 - x_2) \bmod 26 \rightarrow b = \frac{y2x1 - y1x2}{x1 - x2} \bmod 26$

Condition: x_1 and x_2 must be unequal because we need 2 equation to get a , b (key)

Encryption/Decryption

1. Plain text : Sara Baradaran

   Cipher text : Ygxg Hgxgjgxgt

   Shift number = 6

---

2. Plain text : If you cannot explain it to a six year old you do not understand it yourself.

   offset = 9 , key = qhpgiuwaeylnofdxjkrzvstcmb
   Cipher text : Bt xun zkiiul sdwpkbi bl lu k ybd xske upv xun vu iul nivseylkiv bl xuneyspt.

---

3. Plain text : If you cannot explain it to a six year old you do not understand it yourself.
   i. Cipher text with key = iut : Qz rwo vihgwn xfjeicg qn mw u lqr rmuk wfw gin li gwn nvxxzmmihw qn rwokayen.

   ii. Cipher text with key = isfahanuniversityoftechnology : Qx dob cnhawo iohttgb nm xq h fwi mkyz gqd foh xb vjx lflxpgytrf pg mzixqmdk.

   iii. Yes, a longer key makes ciphertext harder for the solver to match up the letter frequencies against the known letter frequencies of English so the vigenere cipher with longer key is stronger than a cipher with shortest key in other words, If very long keys are used the vigenere cipher can be unbreakable but if short keys are used the vigenere cipher is quite solvable.

---

4. Plain text : If you cannot explain it to a six year old you do not understand it yourself.
   i. Cipher text : cg 7jq frsdpz k8xkrp3 ex wk r ap8 zcrb pms 7lw 1w dpu vsnfaaqrsn hq zlwbafkeu.
   Key : Sarbdn962413 (sarabaradaran9624193)
   ii. Plain text : If you cannot explain it to a six year old you do not understand it yourselfx.

s	a	R	b	d	N
9	6	2	4	1	3
c	e	f	g	h	I
j	k	l	m	o	P
q	t	u	v	w	X
y	z	0	5	7	8

Analysis

1.

i. in cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. the receiver deciphers the text by performing the inverse substitution. substitution ciphers can be compared with transposition ciphers. in a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. by contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered. there are a number of different types of substitution cipher. if the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. a monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa.

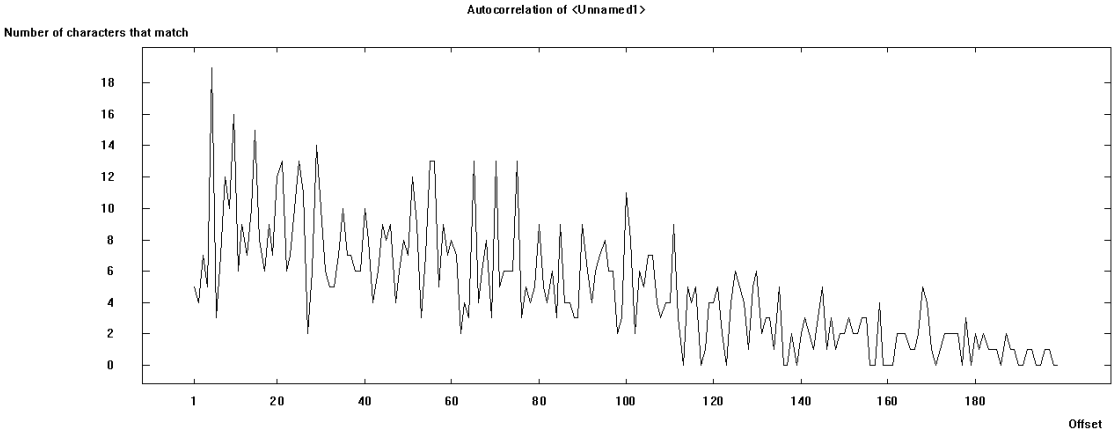
ii. although the traditional keyword method for creating a mixed substitution alphabet is simple, a serious disadvantage is that the last letters of the alphabet (which are mostly low frequency) tend to stay at the end. a stronger way of constructing a mixed alphabet is to perform a columnar transposition on the ordinary alphabet using the keyword, but this is not often done.

Result →The first text is better deciphered because it is long enough to use method which analysis the frequency of diagram in the ciphertext and guesses the key based on standard diagram distribution.

2.

<Key> = smile

deciphered text : cryptool is very flexible and easy to use making it ideal for teaching people about cryptography it also contains several demonstration examples that are designed to be very easy to follow and break down the mathematics into small manageable steps.



---

3. key was not found because of conflict.

   Analysis → Symmetric Encryption (classic) → known plaintext → Hill → Enter plaintext and cipher text