1.1.

The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key.

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

1. Compute the relative frequency of all letters A...Z in the ciphertext. You may want to use a tool such as the open-source program CrypTool [50] for this task. However, a paper and pencil approach is also still doable.

Answer:
Using the analysis from https://www.cryptool.org/en/cto/frequency-analysis , we get following results

cipher character	Amount	Sum of occurences	Frequency Percentages (%)
L	8	646	1.238390093
R	84		13.00309598
V	22		3.405572755
M	62		9.59752322
N	17		2.631578947
I	41		6.346749226
B	68		10.52631579
P	30		4.643962848
S	17		2.631578947
U	24		3.715170279
W	47		7.275541796
J	48		7.430340557
X	20		3.095975232
Y	19		2.941176471
E	5		0.773993808
K	49		7.585139319
Q	7		1.083591331
D	23		3.560371517
T	13		2.012383901
H	23		3.560371517
O	7		1.083591331
A	5		0.773993808
C	5		0.773993808
F	1		0.154798762
G	1		0.154798762

2. Decrypt the ciphertext with the help of the relative letter frequency of the English language (see Table 1.1 in Sect. 1.2.2). Note that the text is relatively short and that the letter frequencies in it might not perfectly align with that of general English language from the table.

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

Cipher text

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi
bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx
ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr
yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk
lmird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi
iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m
vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd
wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr
jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii
ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh
mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb
bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd
wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr
riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

Doing following analysis in excel,

cipher character	Amount	Sum of occurences	Frequency Percentages (%)	Relative frequency of english alphabets sorted	
R	84	646	13.00309598	E	0.127
B	68		10.52631579	T	0.0906
M	62		9.59752322	A	0.0817
K	49		7.585139319	O	0.0751
J	48		7.430340557	I	0.0697
W	47		7.275541796	N	0.0675
I	41		6.346749226	S	0.0633
P	30		4.643962848	H	0.0609
U	24		3.715170279	R	0.0599
D	23		3.560371517	L	0.0403
H	23		3.560371517	D	0.0425
V	22		3.405572755	C	0.0278
X	20		3.095975232	U	0.0276
Y	19		2.941176471	M	0.0241
N	17		2.631578947	W	0.0236
S	17		2.631578947	F	0.0223
T	13		2.012383901	G	0.0202
L	8		1.238390093	Y	0.0197
Q	7		1.083591331	P	0.0193
O	7		1.083591331	B	0.015
E	5		0.773993808	V	0.0098
A	5		0.773993808	K	0.0077
C	5		0.773993808	J	0.0015
F	1		0.154798762	X	0.0015
G	1		0.154798762	Q	0.001
				Z	0.0007

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

We get following transformation

Cipher character	Corresponding english character
R	E
B	T
M	A
K	O
J	I
W	N
I	S
P	H
U	R
D	L
H	D
V	C
X	U
Y	M
N	W
S	F
T	G
L	Y

Q	P
O	B
E	V
A	K
C	J
F	X
G	Q
	Z

And the following text
YECAWSE THE FRACTNCE IU THE YASNC MIVEMEOTS IU PATA NS
THE UICWS AOL MASTERG IU SEDU NS THE ESSEOCE IU
MATSWYAGASHN RGW PARATE LI N SHADD TRG TI EDWCNLATE THE
MIVEMEOTS IU THE PATA ACCIRLNOB TI MG NOTERFRETATNIO
YASEL IO UIRTG GEARS IU STWLG
NT NS OIT AO EASG TASP TI EKFDANO EACH MIVEMEOT AOL NTS
SNBONUNCAOCE AOL SIME MWST REMANO WOEKFDANOEL TI BNVE A
CIMFDETE EKFDAOATNIO IOE JIWDL HAVE TI YE XWADNUNEL AOL
NOSFNREL TI SWCH AO EKTEOT THAT HE CIWDL REACH THE STATE
IU EODNBHTEOEL MNOL CAFAYDE IU RECIBONQNOB SIWOLDESS
SIWOL AOL SHAFEDESS SHAFE N LI OIT LEEM MGSEDU THE UNOAD
AWTHIRNTG YWT MG EKFERNEOCE JNTH PATA HAS DEUT OI LIWYT
THAT THE UIDDIJNOB NS THE FRIFER AFFDNCATNIO AOL
NOTERFRETATNIO N IUUER MG THEIRNES NO THE HIFE THAT THE
ESSEOCE IU IPNOAJAO PARATE JNDD REMANO NOTACT

Looking at above text, we can infer some words like ‘YECAWSE’ should be ‘BECAUSE’, which means we inferred some letters incorrectly
So,

L should be → B (instead of Y)
N should be → U (instead of W)

Same with word “ESSEOCE” should be ESSENCE, which means
K should be → N (instead of O)

Same with word “MIVEMEOTS” (cipher word ‘yjeryrkbi’) should be MOVEMENTS, which means
J should be O (instead of I)
K should be N (instead of O)

Now, our transformed text looks like this

BECAUSE THE FRACTNCE OU THE BASNC MOVEMENTS OU PATA NS
THE UOCUS ANL MASTERG OU SEDU NS THE ESSENCE OU

MATSUBAGASHN RGU PARATE LO N SHADD TRG TO EDUCNLATE THE
MOVEMENTS OU THE PATA ACCORLNNB TO MG NNTERFRETATNON
BASEL ON UORTG GEARS OU STULG
NT NS NOT AN EASG TASP TO EKFDANN EACH MOVEMENT ANL NTS
SNBNNUNCANCE ANL SOME MUST REMANN UNEKFDANNEL TO BNVE A
COMFDETE EKFDANATNON ONE JOUDL HAVE TO BE XUADNUNEL ANL
NNSFNREL TO SUCH AN EKTENT THAT HE COUDL REACH THE STATE
OU ENDNBHTENEL MNNL CAFABDE OU RECOBNNQNNB SOUNLDESS
SOUNL ANL SHAFEDESS SHAFE N LO NOT LEEM MGSEDU THE UNNAD
AUTHORNTG BUT MG EKFERNENCE JNTH PATA HAS DEUT NO LOUBT
THAT THE UODDOJNNB NS THE FROFER AFFDNCATNON ANL
NNTERFRETATNON N OUUER MG THEORNES NN THE HOFE THAT THE
ESSENCE OU OPNNAJAN PARATE JNDD REMANN NNTACT

From above, OU (cipher text “jx”) should be OF, which means
X should be F (instead of U)

Same way, BASNC (ciphertext “lmiwv”) should be BASIC, which means
W should be I (instead of N)

Now our transformed text is

BECAUSE THE FRACTICE OF THE BASIC MOVEMENTS OF PATA IS
THE FOCUS ANL MASTERG OF SEDF IS THE ESSENCE OF
MATSUBAGASHI RGU PARATE LO I SHADD TRG TO EDUCILATE THE
MOVEMENTS OF THE PATA ACCORLINB TO MG INTERFRETATION
BASEL ON FORTG GEARS OF STULG
IT IS NOT AN EASG TASP TO EKFDAIN EACH MOVEMENT ANL ITS
SIBNIFICANCE ANL SOME MUST REMAIN UNEKFDAINEL TO BIVE A
COMFDETE EKFDANATION ONE JOUDL HAVE TO BE XUADIFIEL ANL
INSFIREL TO SUCH AN EKTENT THAT HE COUDL REACH THE STATE
OF ENDIBHTENEL MINL CAFABDE OF RECOBNIQINB SOUNLDESS
SOUNL ANL SHAFEDESS SHAFE I LO NOT LEEM MGSEDF THE FINAD
AUTHORITG BUT MG EKFERIENCE JITH PATA HAS DEFT NO LOUBT
THAT THE FODDOJINB IS THE FROFER AFFDICATION ANL
INTERFRETATION I OFFER MG THEORIES IN THE HOFE THAT THE
ESSENCE OF OPINAJAN PARATE JIDD REMAIN INTACT

From above, FRACTICE (cipher text “sumvbwvr”) should be “PRACTICE”, which means S should be P (instead of F)

SEDF (cipher text “irhx”) should be SELF, which means H should be L (instead of D)

ACCORLINB (ciphertext “mvvjudwko”) should be ACCORDING, which means O should be G (instead of B), D should D (instead of L)

AUTHORITG(ciphertext “mnbpjuwbt”) should be AUTHORITY, which means T should be Y (instead of G)

EKTENT(ciphertext “rabrkb”) should be EXTENT, which means A should be X (instead of K)

JITH (cipher text “cwbp”) should be WITH, which means C should be W (instead of J)

PARATE (cipher text “qmumbr”) should be KARATE, which means Q should be K (instead of P)

Now our transformed text is

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS
THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF
MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE
MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION
BASED ON FORTY YEARS OF STUDY
IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS
SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A
COMPLETE EXPLANATION ONE WOULD HAVE TO BE XUALIFIED AND
INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE
OF ENLIGHTENED MIND CAPABLE OF RECOGNIQING SOUNDLESS
SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL
AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT
THAT THE FOLLOWING IS THE PROPER APPLICATION AND
INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE
ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT

From above,

XUALIFIED (ciphertext “fnmhwxwrd”) should be QUALIFIED, which means F should be Q(instead of X)
RECOGNIQING (cipher text “urvjokwgwko”) should be RECOGNIZING, which means G should be Z(instead of Q)

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF KATA IS
THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF
MATSUBAYASHI RYU KARATE DO I SHALL TRY TO ELUCIDATE THE
MOVEMENTS OF THE KATA ACCORDING TO MY INTERPRETATION
BASED ON FORTY YEARS OF STUDY
IT IS NOT AN EASY TASK TO EXPLAIN EACH MOVEMENT AND ITS
SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A
COMPLETE EXPLANATION ONE WOULD HAVE TO BE QUALIFIED AND
INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE
OF ENLIGHTENED MIND CAPABLE OF RECOGNIZING SOUNDLESS
SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL
AUTHORITY BUT MY EXPERIENCE WITH KATA HAS LEFT NO DOUBT
THAT THE FOLLOWING IS THE PROPER APPLICATION AND
INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE
ESSENCE OF OKINAWAN KARATE WILL REMAIN INTACT

Final result of Cipher char to Corresponding char :
R E
B T
M A
K N
J O

W I
I S
P H
U R
H L
V C
X F
Y M
N U
S P
T Y
L B
Q K
O G
E V
A X
C W
F Q
G Z

3. Who wrote the text?
The above text is found in Essence of Okinawan Karate-Do By Shoshin Nagamine as per https://www.google.com/books/edition/Essence_of_Okinawan_Karate_Do/lirRAgAAQBAJ?hl=en&gbpv=1&dq=Essence+of+Okinawan+Karate-Do&printsec=frontcover .

1.2.
We received the following ciphertext which was encoded with a shift cipher:
xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpit
ghlxiwiwtxgqadds.
1. Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

Answer:
First do the frequency analysis, we get that t is the most occurring character(15% of time) in the ciphertext and the next frequent character is around 13.4%. Most likely, the most frequent character will be the character e. So, because it's a shift cipher and it is 10 shifts away in forward direction from e, we can apply the same 10 shift amount to other characters as well. Using this criteria, we get the following mapping
T E
I T
X I
L W
P A
A L
G R
H S
W H
D O
J U

C N
U F
R C
K V
V G
Q B
S D

If we substitute the above pairs in the ciphertext, we get out deciphered message below "IFWEALLUNITEWEWILLCAUSETHERIVERSTOSTAINTHEGREATWATERSWITHTHEIRBLOOD"

2. Who wrote this message?
This message was written by Tecumseh as per this link: https://en.wikisource.org/wiki/Tecumseh%27s_Speech_to_the_Osages

1.4.
We now consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.

1. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?

Answer: Because each letter can have 128 possible characters, so size of key space will be = 128 x 128 x 128 x 128 x 128 x 128 x 128 x 128 = (128) ^ 8

2. What is the corresponding key length in bits?

Answer: The corresponding key length is 7 bits *8 = 56 bits

3. Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?

Answer: If we are using only 26 lower case letters out of 128 possible characters considering that the every letter is still 7 bits long the key length with still be 7 bits *8 = 56 bits.
But if we are allowed to reduce the no. of bits in ASCII-encoding we can represent any of the 26 lower case letters with just 5 bits, in that case the key length reduces to 5 bits * 8 = 40 bits.
Whereas we cannot represent 26 lower case letters in 4 bits because 2^4 = 16 which is less than 26.

4. At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of
a. 7-bit characters?

b. 26 lowercase letters from the alphabet?

Answer:
a.We would need at least 19 letters in the password, because if we have 18 letters the key length in terms of bits will still be 18*7 = 126 which is less than 128 and for 19 letters the key length will be 133 bits, i.e, 19*7.

b.If we represent the 26 lowercase letters using 5 bit encoding then we will need 26 letters to generate the key length of 128 bits because 26*5 = 130 and 25*5 = 125 which is less than 128.

1.5.
As we learned in this chapter, modular arithmetic is the basis of many cryptosystems. As a consequence, we will address this topic with several problems in this and upcoming chapters. Let’s start with an easy one: Compute the result without a calculator.
1. $15 \cdot 29 \bmod 13$

Answer: (15 mod 13)(29 mod 13) = 2*3 = 6

2. $2 \cdot 29 \bmod 13$

Answer: (2 mod 13)(29 mod 13) = 2*3 = 6

3. $2 \cdot 3 \bmod 13$

Answer: 6

4. $-11 \cdot 3 \bmod 13$

Answer:

-11 is equivalent to 2 since (2 - (-11)) = 13 is divisible by 13. So replacing -11 with 2
= $2 \cdot 3 \bmod 13$ =6

The results should be given in the range from 0,1,..., modulus-1. Briefly describe the relation between the different parts of the problem.

Answer:

It does not matter how many times we add or subtract the modulus value, the remainder value does not change.

For example:

From above statements:

The difference between first and second parts of this problem

$15 \cdot 29 \bmod 13$ AND $2 \cdot 29 \bmod 13$

Is,

If we subtract 13 from the first part (15) of $15 \cdot 29 \bmod 13$
We are left with $2 \cdot 29 \bmod 13$
So, the result for both is 6 and it does not change.
Same with other parts of this problem. So, all have the same result which is 6.

1.6.
Compute without a calculator:
1. 1/5 mod 13
Answer:

1/5 is basically 5^-1 i.e. multiplicative inverse of 5

We know that (5 * (5^-1)) mod 13 is congruent to 1 since gcd(5, 13) is 1, the multiplicative inverse of 5 in mod 13 will exist. After hit and trial, we find the 5^-1 i.e. multiplicative inverse of 5 should be 8 because

5 * 8 mod 13 = 1

So, our answer is 1/5 mod 13 = 8 mod 13

2. 1/5 mod 7
Answer:
1/5 is basically 5^-1 i.e. multiplicative inverse of 5

We know that (5 * (5^-1)) mod 7 is congruent to 1 since gcd(5, 7) is 1, the multiplicative inverse of 5 in mod 7 will exist. After hit and trial, we find the 5^-1 i.e. multiplicative inverse of 5 should be 3 because

5 * 3 mod 7 = 1

So, our answer is 1/5 mod 7 = 3 mod 7

3. 3 · 2/5 mod 7
Answer:
3 · 2/5 mod 7
= (6 / 5) mod 7
= (6 * 5^-1) mod 7

From the above result, multiplicative inverse of 5 mod 7 i.e 5^-1 mod 7= 3.
So,
= (6*3) mod 7
= 4 mod 7

1.7.
We consider the ring Z4. Construct a table which describes the addition of all elements in the ring with each other:

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

1. Construct the multiplication table for Z4.
2. Construct the addition and multiplication tables for Z5.

1. 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

2. Addition & 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. Construct the addition and multiplication tables for Z6.

3. Addition & Multiplication of Z_6

+	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.

×	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

4. There are elements in Z4 and Z6 without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for all nonzero elements in Z5?

In Z4, elements 0 and 2 do not have multiplicative inverses.
In Z6, elements 0, 2, 3 and 4 do not have multiplicative inverses.

Because 5 is a prime number, so gcd of all nonzero elements in Z5 with 5 will be 1. So, all non zero elements will have multiplicative inverse.

1.8.
What is the multiplicative inverse of 5 in Z11, Z12, and Z13? You can do a trial-and-error search using a calculator or a PC. With this simple problem we want now to stress the fact that the inverse of an integer in a given ring depends completely on the ring considered. That is, if the modulus changes, the inverse changes. Hence, it doesn't make sense to talk about an inverse of an element unless it is clear what the modulus is. This fact is crucial for the RSA cryptosystem, which is introduced in Chap. 7. The extended Euclidean algorithm, which can be used for computing inverses efficiently, is introduced in Sect. 6.3.

Answer:
For Z11, since 5 * 9 mod 11 = 1, So, multiplicative inverse of 5 in Z11 is 9

For Z12, since 5 * 5 mod 12 = 1, So, multiplicative inverse of 5 in Z12 is 5

For Z13, since 5 * 8 mod 13 = 1, So, multiplicative inverse of 5 in Z13 is 8

1.9.
Compute x as far as possible without a calculator. Where appropriate, make use of a smart decomposition of the exponent as shown in the example in Sect. 1.4.1:
1. x = 3^2 mod 13
Answer: 9 mod 13

2. x = 7^2 mod 13
Answer: 10 mod 13

3. x = 3^10 mod 13
Answer:
x = ((3^3) (3^3) (3^3) 3) mod 13
= (27)(27)(27)(3) mod 13
= (1)(1)(1)(3) mod 13
= 3 mod 13

4. x = 7^100 mod 13
Answer:
= (7^2)^50 mod 13
= (49)^50 mod 13
= 10^50 mod 13
= (10^2)^25 mod 13
= (100)^25 mod 13
= 9^25 mod 13
= (9^2)^12 (9) mod 13
= (81)^12 (9) mod 13

= 3^12 (9) mod 13
= (3^4)^3 (9) mod 13
= (81)^3 (9) mod 13
= 3^3 (9) mod 13
= (27) (9) mod 13
= 9 mod 13

5. 7^x = 11 mod 13

The last problem is called a discrete logarithm and points to a hard problem which we discuss in Chap. 8. The security of many public-key schemes is based on the hardness of solving the discrete logarithm for large numbers, e.g., with more than 1000 bits.

Answer:

Trying x = 2
7^2 mod 13 = 10

Trying x = 3
7^3 mod 13 = (7^2) (7) mod 13 = 10 * 7 mod 13 = 5

Trying x = 4
7^4 mod 13 = (7^2) (7^2) mod 13 = 10 * 10 mod 13 = 100 mod 13 = 9

Trying x= 5
7^5 mod 13
= (7^2)(7^2) (7) mod 13
= 10 * 10 * 7 mod 13
= 100 * 7 mod 13
= 9 * 7 mod 13
= 63 mod 13
= 11 mod 13, which is what we want

So, our answer is x=5

1.11.
This problem deals with the affine cipher with the key parameters a = 7, b = 22.

1. Decrypt the text below:

falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

Answer:

Multiplicative inverse(a^-1) of a = 15 since 7 * 15 mod 26 = 1 mod 26.

Table 1.3 Encoding of letters for the shift cipher

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

The equation for decryption is

X = (a^-1)(y-b) mod 26

For "F"
X = 15*(f-22) mod 26
X = 15*(5-22+26) mod 26
X = 15*9 mod 26
X = 5

For "Y",
X = (a^-1)(Y-b) mod 26

X = 15*(24-22) mod 26
X = 15*2 mod 26
X = 4

For "Z",
X = (a^-1)(Z-b) mod 26
X = 15*(25-22) mod 26
X = 15*3 mod 26
X = 19 -> T

For "J",
X = (a^-1)(J-b) mod 26
X = 15*(9-22) mod 26
X = 15*(9-22+26) mod 26
X = 15*13 mod 26
X = 13 -> N

For "T",
X = (a^-1)(T-b) mod 26
X = 15*(19-22) mod 26
X = 15*(-3+26) mod 26
X = 15*23 mod 26
X = 7 -> H

For "A",
X = (a^-1)(A-b) mod 26
X = 15*(0-22) mod 26
X = 15*(-22+26) mod 26

X = 15*4 mod 26
X = 8 -> I

For “S”,
X = (a^-1)(S-b) mod 26
X = 15*(18-22) mod 26
X = 15*(-4+26) mod 26
X = 15*22 mod 26
X = 18 -> S

For “R”,
X = (a^-1)(R-b) mod 26
X = 15*(17-22) mod 26
X = 15*(-5+26) mod 26
X = 15*21 mod 26
X = 3 ->D

For “K”,
X = (a^-1)(K-b) mod 26
X = 15*(10-22) mod 26
X = 15*(-12+26) mod 26
X = 15*14 mod 26
X = 2 ->C

For “W”,
X = (a^-1)(W-b) mod 26
X = 15*(22-22) mod 26
X = 15*(0) mod 26
X = 0 mod 26
X = 0 -> A

For “L”,
X = (a^-1)(L-b) mod 26
X = 15*(11-22) mod 26
X = 15*(-11+26) mod 26
X = 15*15 mod 26
X = 17 -> R

For “N”,
X = (a^-1)(N-b) mod 26
X = 15*(13-22) mod 26
X = 15*(-9+26) mod 26
X = 15*17 mod 26
X = 21 -> V

For “E”,
X = (a^-1)(E-b) mod 26
X = 15*(4-22) mod 26
X = 15*(-18+26) mod 26

$X = 15*8 \mod 26$
$X = 16$ -> Q

So, using above mappings are
FF
YE
ZT
JN
TH
AI
RD
KC
WA
LR
NV
EQ

And the deciphered text after substituting for above pairs is

“FIRSTTHESENTENCEANDTHENTHEEVIDENCESAIDTHEQGEEN”

2. Who wrote the line?
The line is a quote in Lewis Carroll's Alice's Adventures Under Ground - Pages 88 and 89 as per https://www.bl.uk/onlinegallery/ttp/alice/accessible/pages88and89.html#:~:text=%22No!%22%20said%20the%20Queen,tongue!%22%20said%20the%20Queen.

1.12.
Now, we want to extend the affine cipher from Sect. 1.4.4 such that we can encrypt and decrypt messages written with the full German alphabet. The German alphabet consists of the English one together with the three umlauts, A, ¨ O, ¨ U, and the ¨ (even stranger) “double s” character ß.
We use the following mapping from letters to integers:
A ↔ 0 B ↔ 1 C ↔ 2 D ↔ 3 E ↔ 4 F ↔ 5 G ↔ 6 H ↔ 7 I ↔ 8 J ↔ 9 K ↔ 10 L ↔ 11 M ↔ 12 N ↔ 13 O ↔ 14 P ↔ 15 Q ↔ 16 R ↔ 17 S ↔ 18 T ↔ 19 U ↔ 20 V ↔ 21 W ↔ 22 X ↔ 23 Y ↔ 24 Z ↔ 25 A¨ ↔ 26 O¨ ↔ 27 U¨ ↔ 28 ß ↔ 29

1. What are the encryption and decryption equations for the cipher?

Answer:
Encryption:
$Y = (a*x + b) \mod 30$
Decryption:
$X = a^{-1}*(y-b) \mod 30$

2. How large is the key space of the affine cipher for this alphabet?
Answer:
Values of a which have multiplicative inverse in Z30 are {1, 7, 11, 13, 17, 19, 23, 29}. So, there are 8 possible values of a. Other values do not have a multiplicative inverse in Z30.

Number of possible values of b are 30 i.e from 0 to 29.

So, length of possible key space is 8*30 = 240.

There is an edge case in this. When a=1 and b=0, then our encryption equation is y = (1*x + 0) mod 30 i.e. y= x which does not do any encryption. So, we can remove this key from our answer count.
So, we are left with 239 keys.
So, our answer is 239.

3. The following ciphertext was encrypted using the key (a = 17,b = 1). What is the corresponding plaintext?
¨außwß

Number representation of this text is (26, 20, 29, 22, 29)

Decryption equation:

X = (a^-1)*(y-b) mod 30

Using trial and error, we calculate multiplicative inverse(a^-1) of a=17 is 23 since 17*23 mod 30 = 1.
So a^-1 = 23

Substituting in above equation
For ¨a=26,
X = 23 * (26-1) mod 30
X = 23 * 25 mod 30
X = 5 -> F

For u = 20,
X = 23 * (20-1) mod 30
X = 23 * 19 mod 30
X = 17 -> R

For ß=29,
X = 23 * (29-1) mod 30
X = 23 * 28 mod 30
X = 14 -> O

For w=22,
X = 23 * (22-1) mod 30
X = 23 * 21 mod 30
X = 3 -> D

For ß=29,
X = 23 * (29-1) mod 30
X = 23 * 28 mod 30
X = 14 -> O
So, our deciphered text is FRODO.

4. From which village does the plaintext come?
FRODO comes from the Shire as per https://en.wikipedia.org/wiki/Frodo_Baggins