Workshop 1 – Classic Ciphers

Task 1. Review the following concepts and questions

1. List and briefly define categories of passive and active security attacks.

Answer:

Passive Attacks

Passive attacks are to do with unauthorized access to information on communication networks. It involves acquiring information from captured packets in network transmissions. A passive attack can be done to prepare for active attacks. e.g intercepting telnet traffic to obtain passwords of a router.

One type of passive attack is the release of messages

Passive attacks involve capturing a network packet, downloading it and then analyzing it.

The second type of passive attack is traffic analysis, this is where the attacker analyses the traffic flow. The attacker may observe TCP or IP packets or format of packets, this analysis reveals what the network is doing.

Traffic analysis can be used to figure out network topologies for example which router is the root for select VLANS, or figure the root bridge and priorities of routing devices through traffic flow etc.

With passive attacks no immediate harm is caused to the communication of the network

Active Attacks

Active attacks can have many forms, generally these classified as masquerading, replay, modification of messages and denial of service attacks

Masquerading – pretend to be another entity, a good example of this may be an attackers device replying to an ARP request to connect to the network and intercept messages.

Replay – Retransmit data that has been previously obtained in a passive attack. This could be to show credentials of a legitimate victim (user), or done as a step before masquerading, etc.

Modification of messages – Capture, modify, delete or add, then send the captured packet. This form of attack can be done after to send broadcasts while masquerading as a server, etc.

Denial of Service – Prevents normal service, for example flooding a server with a lot of requests than it can handle.

2. List and briefly define categories of security services.

Answer:
The general categories of security services are, Authentication, Access Control, Data Confidentiality, Data Integrity, Non-repudiation, Availability services

Authentication is concerned with verifying authorized users, that is verify you are the authorized user registered in the server's database. In other words this concerns transfer of data between the right entities, by not allowing unauthorized people connecting to the bank server on behalf of an authorized user, this can also be considered as a security measure against masquerading. This is usually accomplished using username and passwords.

Authentication is concerned with users within the system and users outside the system. For external users this includes verifying to access the systems and its services using user password and credentials. Authentication within the system is concerned with authorized staff with appropriate access privileges which defines their access level authorities.

Access Control concerns with user privileges so authorized users can not have unauthorized access to resources, instead access resources granted to them according to access privileges.

Data confidentiality is concerned with protecting user data in a connection. A good example of this could be storing user passwords as hashed strings rather than plain text in the servers database.

Data integrity services ensure data remains unchanged and intact to be delivered as intended by the senders such as servers. This includes protecting stored data from attackers (this could be storing data in encrypted format where only the middleware services can interpret data).This also includes protecting transmitted data from being intercepted and modified, so what is sent is what is received, an example to accomplish this could be using checksums and encryption along with resend and acknowledge messages by the client to the server.

Non-repudiation is concerned with preventing the denial by users or hosts of transmitting or receiving data in the network.

Availability security measures involves design tactics that the server is always available to handle client requests.

3. What is the difference between symmetric-key cipher and asymmetric-key cipher?

Answer:

Symmetric-key ciphers is where the encryption and decryption key are somewhat the same or equivalent.

Both encryption and decryption keys in symmetric ciphers are essentially the same, in the sense that one key can be derived from the other, even if they are not exactly the same. An example of this is the Caesar cipher encoder where the decryption key is the inverse operation of the encryption key.

Symmetric keys are not necessarily codified syntactically, however logically knowing one reveals the other.

Asymmetric-key ciphers use asymmetric conversion techniques, where the encryption and decryption keys are not the same.

One key is used for encryption and another separate key for decryption.

An example of this is two hosts A and B, they both need to securely exchange their public keys to the other host to exchange encrypted messages with asymmetric encryption. This means the sending host encrypts data using the client hosts public key, so for example host A encrypts data using host B's public key, this encrypted data can only be decrypted by host B's private key which should be in the possession of host B only.

4. What is brute-force attack for ciphers?

Answer:

Brute force attacks are where the attacker tries every possible key on a intercepted cipher text until a meaningful decoding to plain text is obtained.

For example for a 128 bit key where the range of values is anywhere between 0x000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000

to

0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

The possible values range from 0 to 2^{128}, only one of all the possible combinations will work.

Another example is the Caesar cipher key can be shifted 0 to 27 places, practically 1 to 26 including the space (ASCII 0x20) character.

Task 2. Reviewing concepts of security services

Consider an Internet banking system that you use. Give examples of confidentiality, integrity, authenticity, and availability requirements associated with the system.

(Normally, an Internet banking system allows to 1) managing online payments and transactions 2) managing (storing, protecting) financial data and account information. Think about the potential attacks, and the security service should be included to defend against such attacks.)

Answer:

Confidentiality measures are concerned in two respects, the network communication with clients as well as the local database in the system.

Confidentiality in network communications involve the verification of authorized clients (i.e. authentication services) before disclosing transaction and account details. This includes secure communication channels and encrypted transmissions after client verification.

Confidentiality is also relevant in the local database within the system, an example of this is storing client passwords as hash data rather than the original password text. If hackers obtain such data the obtained data would not serve hackers as such data is only useful for verification only.

Integrity involves design decisions that make sure data in unchanged and remains intact. Integrity design tactics ensure to prevent attackers to access or modify stored data as well as prevent transmitted data from being intercepted and modified. Integrity ensures the data received by the end user is the same as the data sent by the server.

Integrity also includes preserving the integrity of data from possible sources of corruption within the system apart from external hackers, e.g. Software problems.

Authenticity requirements involve the transfer of data between the bank system and the right persons. This involves preventing unauthorized people from connecting to the bank server on behalf of or pretending as the authorized person, that is also a security measure against masquerading.

With respect to network communications from the bank to the clients, this involves verification via user credentials e.g. passwords. However within the banking system, authentication is concerned with authorized staff having access to parts of the system database depending on their access privileges.

Availability requirements involve design tactics that employ security measures to ensure the system or the server is always available to serve requests of client devices.

Task 3. Attacking Caesar cipher

Decrypt the following Caesar Ciphertext. You can use brute-force attack or statistical cryptanalysis. But do not use any automatic tool.

Ciphertext: PACGHJUHHCRICGRFWRUCRICPHGLFLQH

Answer:

” MY DEGREE OF DOCTOR OF MEDICINE”
Using the alphabet as ciphertext with a space character appended after “z” that is “abcdefghijklmnopqrstuvwxyz “

Using a brute force attack of up to 27 possibilities in theory, however 26 different keys in practice

The weakness of the Ceaser cipher is that knowing one element of the ciphertext means you can map the rest of the sequence of the cipher text encryption mapping, because the alphabet is not random (A to Z). This is because this ciphering technique is simply based on shifting the known alphabet sequence. For this reason the next evolution to the caesar cipher is the random substitution cipher.

See appendix A for the method.

Task 4. Random substitution cipher

Using the 27-character plaintext alphabet of abcdefghijklmnopqrstuvwxyz*, answer the following questions about random substitution cipher.

1. How many possible keys for the substation cipher on the given alphabet?

Answer:

With each possible combination of characters the first character is theoretically 27 (26 letters and the space character), and one less for each following character, the possible number of combinations is the product of each of these character possibilities as illustrated below:

Possible keys = 27 × (27-1) × (27-2) × (27-3) × ….
= 27!
= 10,888,869,450,418,352,160,768,000,000

See Appendix B

2. Given the following encryption key of the substitution cipher, what is the decryption mapping?

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

Answer:

As the substitution cipher like the caeser cipher is one of the simplistic symmetric encryption techniques, the decryption mapping is the inverse function of the encryption mapping. The decryption mapping is the above table with the rows swapped around. So if encryption is mapping the bottom row to the top, decryption is mapping the top row to the bottom.(*See Appendix C for illustration*.)

Although random substitution cipher is one evolution after the Caesar cipher, it is still not a secure method of encryption as there is a one-to-one mapping between plaintext and the ciphertext, which does not protect the message from statistical cryptoanalysis.

And this is because substitution cipher is inadequate, because the ciphertext preserves the statistical pattern of plaintext as it is found in the original plain text due to the usage of natural language.

Task 5. Statistical cryptanalysis

Use Cryptool 1 (or any other similar tools) to display the distribution of characters from any English document (you can choose any document and import to Cryptool 1 or use the file from the "reference" folder of the directory installs Cryptool 1). Answer the following questions:

(Cryptool 1 download link: https://www.cryptool.org/en/ct1/)

1. What is the distribution (i.e., the probability each letter appears in the document)? Take a screenshot of the result. How does it compare to the values of the table from lecture slides? (Take a screenshot of the result.) How does it compare against the letter frequency table given by the lecture slides? (You can use any letter frequency counter. Not necessary Cryptool 1.)

Answer:

Statistical cryptoanalysis remains to be a highly effective starting point. The analysis for this section was carried out as follows:

A sample text was downloaded from the link shown below to get an equal distributed sample space of characters as commonly used in the English language.
https://github.com/crista/exercises-in-programming-style/blob/master/pride-and-prejudice.txt

Three samples were derived using the above text.

- The first sample was the full text
- The second sample contained approximately half of the original text,
- The Third sample contained a quarter of the original text

The findings are as follows:

Full text statistical analysis:

N-gram tables

Rank	1-gram	Abs.	Rel.
1	E	71194	12.062
2	T	48159	8.160
3	A	42695	7.234
4	O	41377	7.010
5	I	38944	6.598
6	N	38721	6.560
7	H	34582	5.859
8	S	33871	5.739
9	R	33467	5.670
10	D	22843	3.870
11	L	22071	3.739
12	U	15512	2.628
13	M	15124	2.562
14	C	14059	2.382
15		13425	2.275
16	Y	13033	2.208
17	W	12573	2.130
18	F	12381	2.098
19	G	10445	1.770
20	B	9362	1.586
21	,	9278	1.572
22	P	8683	1.471
23	.	6396	1.084
24	V	5840	0.989
25	"	3554	0.602
26	K	3342	0.566
27	;	1539	0.261
28	-	1191	0.202
29	J	970	0.164
30	Z	938	0.159

Half text statistical analysis:

N-gram tables

Rank	1-gram	Abs.	Rel.
1	E	35370	11.974
2	T	23854	8.076
3	A	21516	7.284
4	O	20423	6.914
5	I	19867	6.726
6	N	19722	6.677
7	S	17132	5.800
8	H	17116	5.795
9	R	16482	5.580
10	D	11417	3.865
11	L	11233	3.803
12	M	7711	2.611
13	U	7654	2.591
14	C	7138	2.417
15		6771	2.292
16	Y	6730	2.278
17	F	6207	2.101
18	W	6050	2.048
19	G	5197	1.759
20	,	4638	1.570
21	B	4625	1.566
22	P	4283	1.450
23	.	3253	1.101
24	V	2980	1.009
25	"	1979	0.670
26	K	1597	0.541
27	;	729	0.247
28	-	612	0.207
29	Z	466	0.158
30	_	464	0.157

Quarter text statistical analysis:

N-gram tables

Rank	1-gram	Abs.	Rel.
1	E	15987	11.933
2	T	10683	7.974
3	A	9673	7.220
4	I	9118	6.806
5	O	9053	6.757
6	N	8879	6.627
7	S	7717	5.760
8	H	7678	5.731
9	R	7370	5.501
10	D	5301	3.957
11	L	4958	3.701
12	M	3573	2.667
13	U	3486	2.602
14		3228	2.409
15	C	3097	2.312
16	Y	3089	2.306
17	F	2688	2.006
18	W	2686	2.005
19	G	2415	1.803
20	B	2251	1.680
21	,	2182	1.629
22	P	1910	1.426
23	.	1576	1.176
24	V	1309	0.977
25	"	1142	0.852
26	K	742	0.554
27	-	358	0.267
28	;	354	0.264
29	_	264	0.197
30	J	213	0.159

2. How do you think the difference would affect the statistical analysis?

Answer:

The three samples in part 1 showed the most commonly occurring character was the letter “E”.

All three samples show that if a large enough volume of writing is encrypted, with the standard usage of the English language there should be four clusters of characters.

According to this activity, which only samples the same document in three ways (hence not the subject of professional statistical analysis, but done for the purpose of this report only).

The most common group of letters was {E, T, A}
The second common group of characters were {H, I, N, O, R, S}
The third most occurring set of characters were {B, G, J, K, P, Q, V, X, Z, F, W}

The findings of this activity correlated with the graph shown on page 43 of lecture 1 for 3809ICT of 2022.

This activity shows that substitution cipher is inadequate because the cipher text preserves the pattern of the plain text as found in the original plain text.

Hence why the next evolution of cryptography was the Vigenère Cipher.

3. Use Cryptool 1 to conduct cryptanalysis on the following ciphertext from a random substitution cipher. Do not take space into account. Tell your idea and the steps.

FJLTXCFWKOVLHKJVKCBCOTEEVLPKCKJVJSTWTJYVKJVOJSTSBPLVITWCWPVDBITWICKTK
QLVPHYTPRBJSTQLVYTKKJSCJETSCGTUHKJPTKYLFRTPETXCBTKJFXCJTJSTGCZHTVOCGVZJ
CXTJTLCJCSHWPLTPOLCWYKFOJSTCQQCLCJHKVQTLCJTKEFJSVHJCQQLTYFCRZTETCLJSTC
XVLJFATXTWJKSVHZPRTYCZYHZCJTPCJCGTLBZVEOFIHLTKCBQTLYTWJESFYSFKZCLITFWY
VWJFWHVHKVQTLCJFVWFJEVHZPQLVPHYTXVLTJSCWYHRFYXTJTLKVOICKCBTCLKCBCZFJ
JZTZTKKJSCWVWTYTWJFXTQTLYHRFYXTJTLJSTYCHKJFYKVPCFKYVWKJCWJZBLTYHQTLCJ
TPCWPFKWTGTLPTKJLVBTPJSTKVZTQLVPHYJJSCJPFKCQQTCLKFKJSTPFKJFZZTPECJTLWVE
VWTYHRFYXTJTLVOECJTLQLVPHYTKXVLTJSCWYHRFYXTJTLKVOICKJSTTDQTWKTFWECJT
LJSTWPVTKWVJCXVHWJJVCYTWJFXTQTLYHRFYXTJTLJSTILTCJOCYJVLVOJSTTDQTWKTLT
KFPTKFWJSTTZTYJLFYTWTLIBJSTYVKJVOKHLGTFZZCWYTEFZZRTXFWFXHXCWPJSTITWTL
CZTDQTWKTKCPZFRFJHX

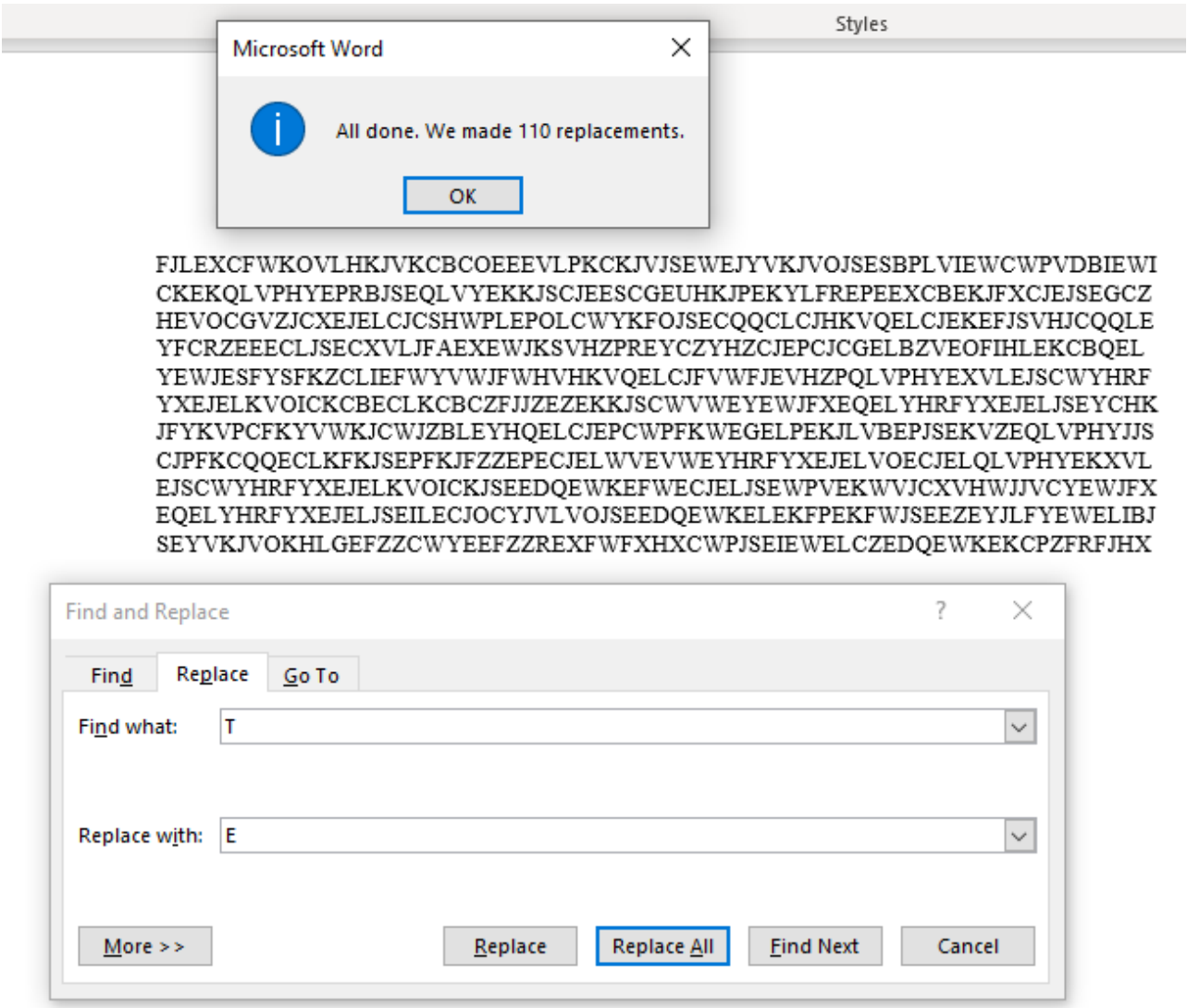
Answer:

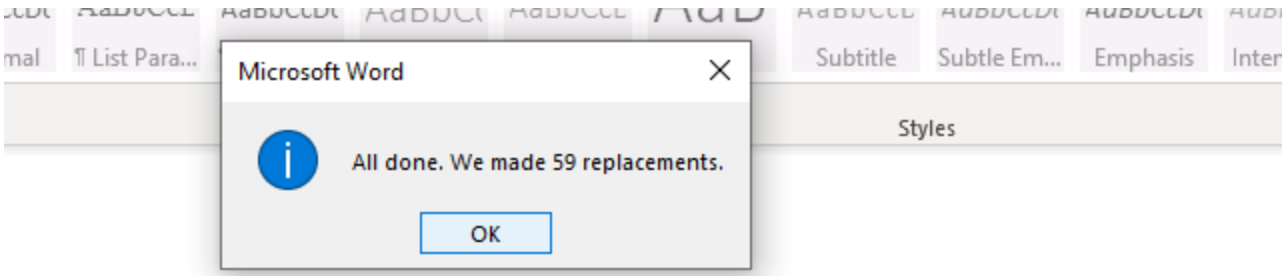
A statistical analysis provided the following results:

N-gram tables

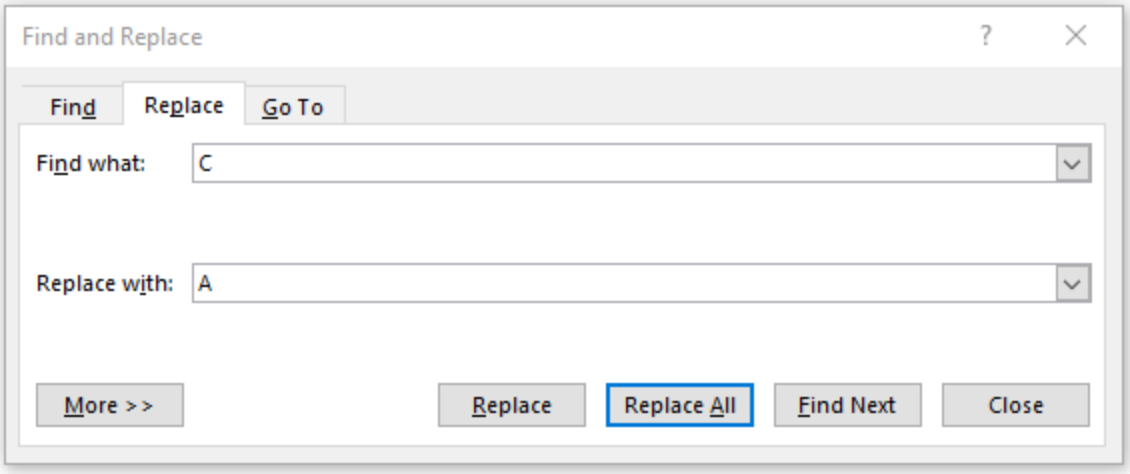
Rank	1-gram	Abs.	Rel.
1	T	110	15.428
2	J	73	10.238
3	C	59	8.275
4	L	48	6.732
5	K	48	6.732
6	V	45	6.311
7	F	40	5.610
8	W	38	5.330
9	Y	35	4.909
10	S	28	3.927
11	H	27	3.787
12	P	27	3.787
13	Z	23	3.226
14	X	20	2.805
15	Q	20	2.805
16	E	14	1.964
17	O	13	1.823
18	B	12	1.683
19	R	11	1.543
20	I	10	1.403
21	G	6	0.842
22	D	4	0.561
23	U	1	0.140
24	A	1	0.140

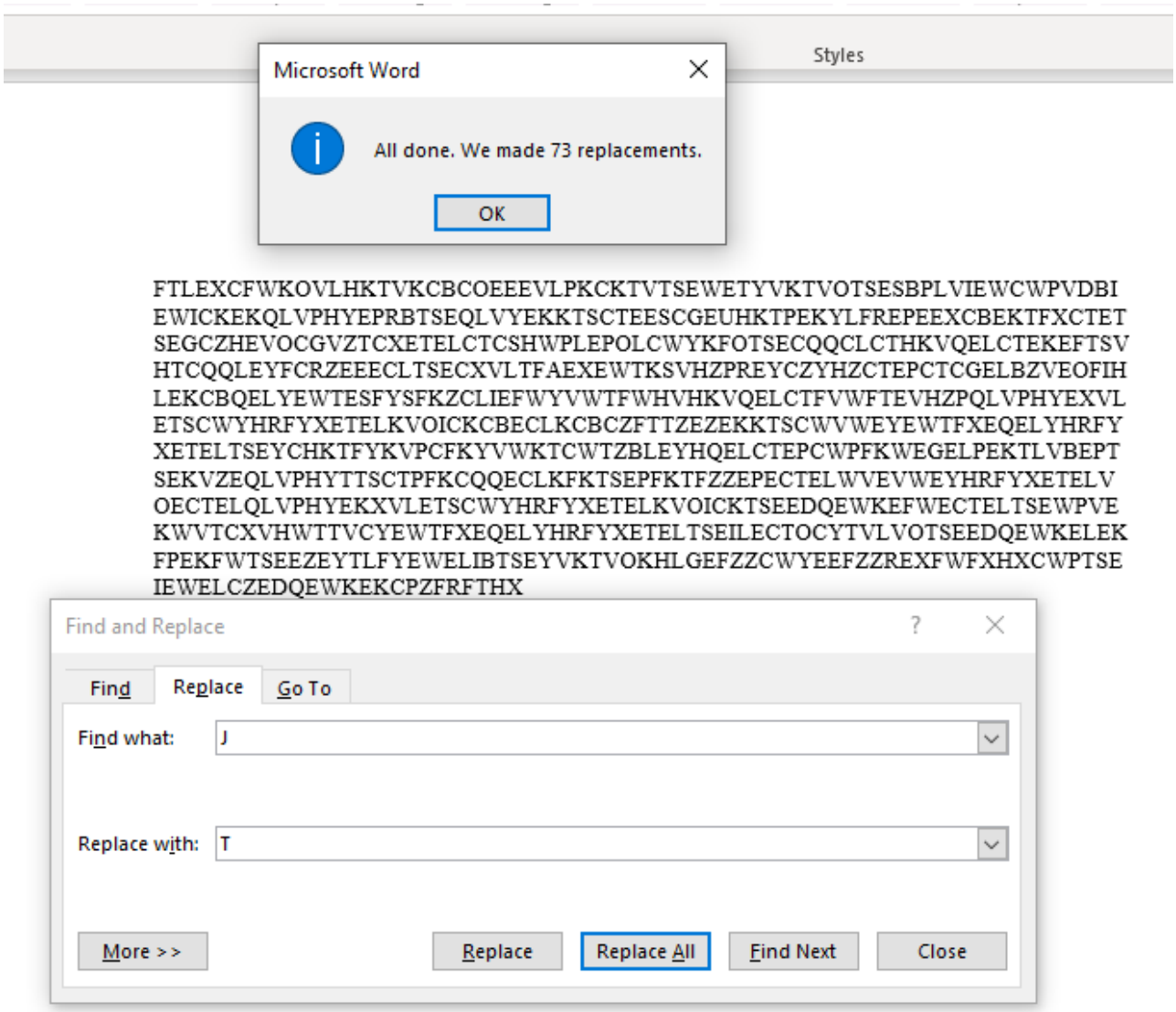
As a result, the table above was used to organize the results and group them into clusters outlined by part 2 of task 5 above, with the first cluster being {E, T, A} as follows:





FTLEXAFWKOVLHKTVKABAOEEEVLPKAKTVTSEWETYVKTVOTSESBPLVIEWAWPVDBI
EWIAKEKQLVPHYEPRBTSEQLVYEKKTSATEESAGEUHKTPEKYLFREPEEXABEKTFXATE
TSEGAZHEVOAGVZTAXETELATASHWPLEPOLAWYKFOTSEAQQALATHKVQELATEKEFT
SVHTAQQLEYFARZEEEALTSEAXVLTFAEXEWTKSVHZPREYAZYHZATEPATAGELBZVEO
FIHLEKABQELYEWTESFYSFKZALIEFWYVWTFWHVHKVQELATFVWFTEVHZPQLVPHYE
XVLETSAWYHRFYXETELKVOIAKABEALKABAZFTTZEZEKKTSAWVWEYEWTFXEQELY
HRFYXETELTSEYAHKTFYKVPAFKYVWKTAWTZBLEYHQELATEPAWPFKWEGELPEKTL
VBEPTSEKVZEQLVPHYTTSATPFKAQQEALKFKTSEPFKTFZZEPEATELWVEVWEYHRFYX
ETELVOEATELQLVPHYEKXVLETSAWYHRFYXETELKVOIAKTSEEDQEWKEFWEATELTS
EWPVEKWVTAXVHWTTVAYEWTFXEQELYHRFYXETELTSEILEATOAYTVLVOTSEEDQE
WKELEKFPEKFWTSEEZEYTLFYEWELIBTSEYVKTVOKHLGEFZZAWYEEFZZREXFWFXH
XAWPTSEIEWELAZEDQEWKEKAPZFRFTHX





The process taken above was to replace the most commonly occurring character of the ciphertext with characters they correlate to in the English language in term of their statistical percentage proportion.

The process was continued the same way for the remaining clusters in order to decode the original message, however no meaningful result was achieved.

The conclusion reached was, the findings may be the case because the ciphertext provided is only a small sample. The second reason is assumed that my manual approach did not exhaust all possible combinations for each cluster of letters, especially the last cluster (i.e {B, G, J, K, P, Q, V, X, Z, F, W})

For this reason the second approach with breaking the encryption was to use the site https://guballa.de/substitution-solver, where the results were much more meaningful:

ITREMAINSFORUSTOSAYAFEWWORDSASTOTHENETCOSTOFTHEHYDROGENANDOX
YGENGASESPRODUCEDBYTHEPROCESSTHATWEHAVEJUSTDESCRIBEDWEMAYESTI
MATETHEVALUEOFAVOLTAMETERATAHUNDREDFRANCSIFTHEAPPARATUSOPERA
TESWITHOUTAPPRECIABLEWEARTHEAMORTIZEMENTSHOULDBECALCULATEDAT
AVERYLOWFIGURESAYPERCENTWHICHISLARGEINCONTINUOUSOPERATIONITWOU
LDPRODUCEMORETHANCUBICMETERSOFGASAYEARSAYALITTLELESSTHANONECE
NTIMEPERCUBICMETERTHECAUSTICSODAISCONSTANTLYRECUPERATEDANDISNE
VERDESTROYEDTHESOLEPRODUCTTHATDISAPPEARSISTHEDISTILLEDWATERNOW
ONECUBICMETEROFWATERPRODUCESMORETHANCUBICMETERSOFGASTHEEXPEN
SEINWATERTHENDOESNOTAMOUNTTOACENTIMEPERCUBICMETERTHEGREATFAC
TOROFTHEEXPENSERESIDESINTHEELECTRICENERGYTHECOSTOFSURVEILLANCEW
ILLBEMINIMUMANDTHEGENERALEXPENSESADLIBITUM

Task 6. Vigenère Cipher

Download the two ciphertexts files which are encryptions using Vigenère Cipher.

1. Using Cryptool 1 to display the letter distributions. Compare the distribution with the English text distribution given in the lecture slides. Are they different? Why?

Answer:

They are different as we see from the Vigenère cipher,where “S” maps to both “L” and “O” in different instances depending on which element of the key is used to map the plain text character to the corresponding cipher letter.

This is a very good demonstration of how the Vigenère cipher shows the distribution of characters where the cipher text character distributions do not correlate with the relative frequency of English text statistics but rather repetitions are based on the frequency of the key used in the encryption, which is not shared with the attacker. So we see the following:

Frequency of Cipher text ! ≡ frequency found in English text statistics

2. One practical cryptanalysis against Vigenère Cipher is autocorrelation analysis. Autocorrelation identifies correlations (statistical relationships) between a string and the shifts of that string. Using the automatic tool from Cryptool 1 to decrypt the following ciphertexts. Discuss why autocorrelation helps.

Answer:

Autocorrelation analysis is useful because the Vigenère cipher is effectively a rotating (or periodic) substitution cipher. Rather than looking at the whole text for statistical correlation with respect to the distribution ratio of the letters in English text (as we would for the Caeser or substitution copher), we look for periodic repetitions, that is the repetition of the secret key. If we know the character size of the key, in other words the number of characters in the key, then we can break up the cipher text into chunks of that key size.

With this understanding it is possible to observe the characters as chunks of cypher encryptions.

For the example in lecture one, if you extract every four columns of characters consecutively and treat every column as 4 a character substitution cipher text, based on the size of the key (i.e. "WHAT"). Knowledge of the size of the key, and the fact the same key is repeating is a pattern that is a starting point to investigate a decryption strategy.

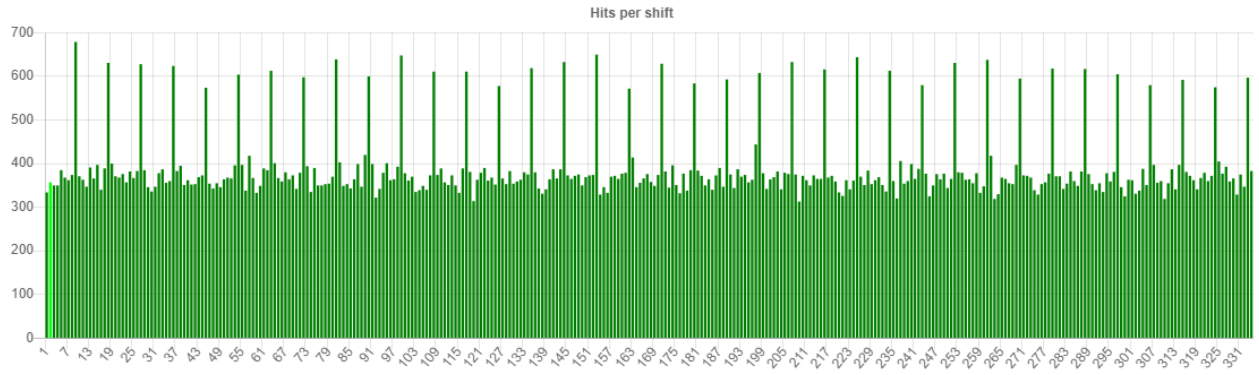
Autocorrelation helps the cryptanalyst find the repeating sequence that reveals the size of the key, which is every chunk of substitution cipher pieces.

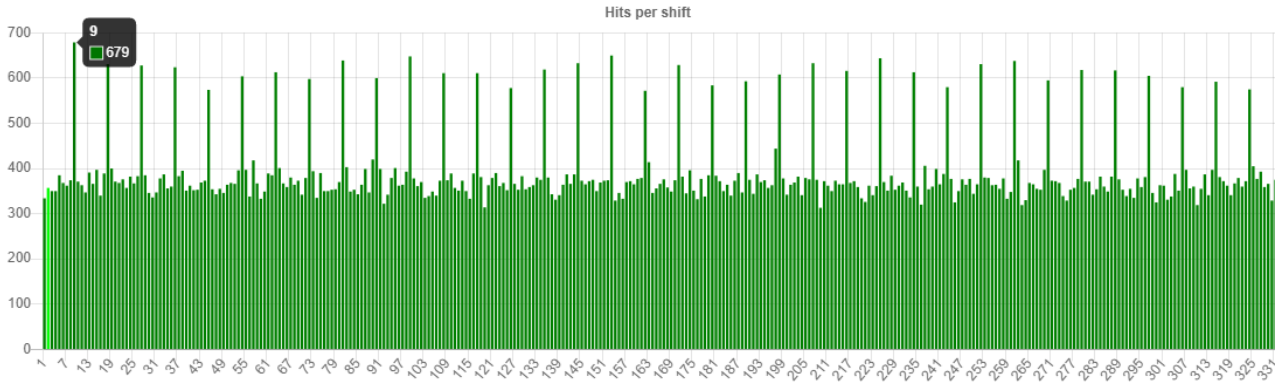
For this section the file named "*Cry-Vigenere-Ciphertext1.txt*" was used for autocorrelation. The result was a perfect distribution of peak points after every 9^{th} sequence.

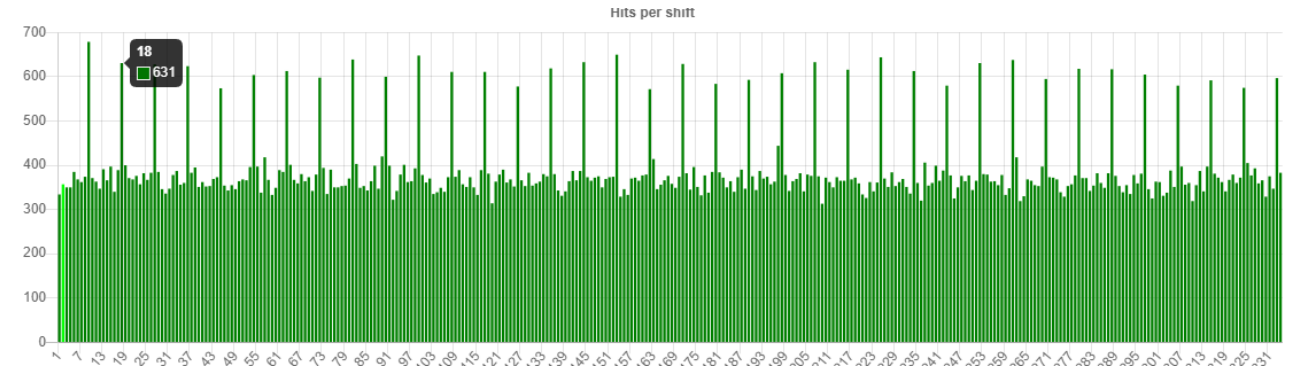
CrypTool-Online
Cryptography for everybody

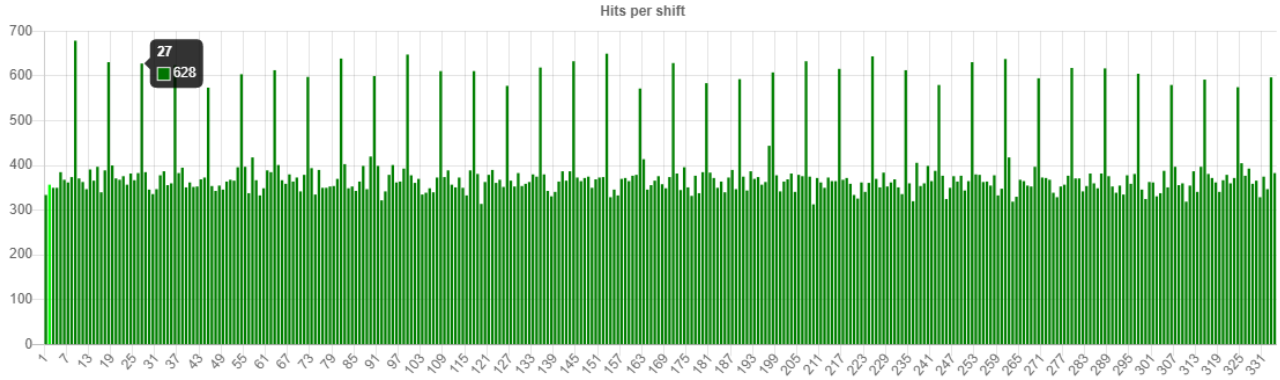
csrtjtreslppfjwbhpwqifjbbnphhvwjacsnzvxvvspmjdxiebwpmjdxiejvsmcwiqelgynelqeaxtnrfnmwrvwldfgmhrwhjyboefouspiodgmrwqcmsssspzngypjnoieddmftsip
ybcltipwlbasqogelitasytvyorbfbmcflrmcasqunpxlncwritxvwunfjodvlsyvsqwizqmnvobdspwwvwuyneysxaxhfittwqlofgeoohvjjhqoorpeqcckefecshbwpiilziunopdz
zyvajacmfyxmbwsbionsranqripyamgqhfauzjcbdfdrjprhlxignupvifcagvfccqhlvkrizpqrbwfaesevqumcxqpgxrmgmdpwmguxqcpilpmpjgiumwsvfdqfwfwpqnaycdtft
vnxfziulphresjoqxirgfcslejsyujjcaojsfwnqripyxszhfsnotrkzhtgnhpveyxbeypfvtnawctbwjmfbipebnewgxtwovcwohuzqisfrxvuhfepcmkvwojitlzevuozlfhsyympcaoz
vrnvsltuzerljbrhsztsyxugcbwqyfnikjutwrbcawioeirgrcltpmijhugmmfmyxvlcffdwxujhgcpgixlxipslfppfqsplpnolbuacsxlziqxipsucertnjgsjesvvwhmadsemehcsaspe
rrwhfuttewgrbwovcpmancdtizykucwnesnimlnggrbdmezrbkiopwevmvcipmwieesdrpxcshatmrfqmrtnfrhbecshvoiezzyvbfbaihlvigcsqhbgirbqsqiulxmbwwlljrlxvw
umnfelizjbbrfhsygyonesIrhgxpycdzerqckgrmphxunclevamrgqsmtipvavcvqusavmfrbedfixlerhwhfsehyxbeqvtzierbefjykieboqahtpinwrpetepifboqtipergnbloglrm
absatizpqrbkysttpiacpstitwpvchjeelvxvwuelbygifbvmwfoqigqsgnupvifckfidsligxciiozyvpdfgovdgszyolipymtengsmfdmvfjwbhflxpnbhrhbemxjjglouxivrumdoselic
dfnotpsjrgokiotrkzhgiumwxlncmmuilziqxbcmfeliuxbmusesgnuzfesppefcbggieerqjuyioeshnhbmsjcrsgqcsgitequjdnyuzleinvydusiscycptvymxlxtbojykxujhysxppp
vlokeuzcshvffomxiwonqyutpmvrlcenjkihgqoribxqcfnzdaofrtejqridlpqnwoldcpgehbsgandyhqnbjydzrjexbreehmxujamsudivvxiqaooibgaomretreehdpocwiqenqm
gotdmapoqiezxlncmmubcixungccpyhlvpvcsupbtrahgnffvscnwldfphwvaayyjtruhrfcwizlefcvchpysyecczeusijvagratvihuxzkethmxubckebdtierhwtpelizjbmfqcigvb
sjytnmiacwdidxmrqcvcwpcossvclsjpyvonfrimwsrzdgramhecfjdnebwwxexbelzeliaqobypfrsgksrtfcgsabijtitqmfjwbsjcxsgqsnrfnmwrumqcjprxvowamjyhfhcoqaqc
eggrqylnlrssjtdajcwmgrgyclysaynreeeeleghcssulrhnuclejevyfcggrusexvqoteozxmajrtesgirgumhuteepvchjetlmhuxzkettxlvwybrnzvxvvspypfashurboxtwiyhwdw
jelshcamrflhslxiuovwhovwrjyuppzndjajypcjqortipibnlhlaufvibohfeqcsfynagsjyalvlvwovoiqnwrkybdwmfcolcf

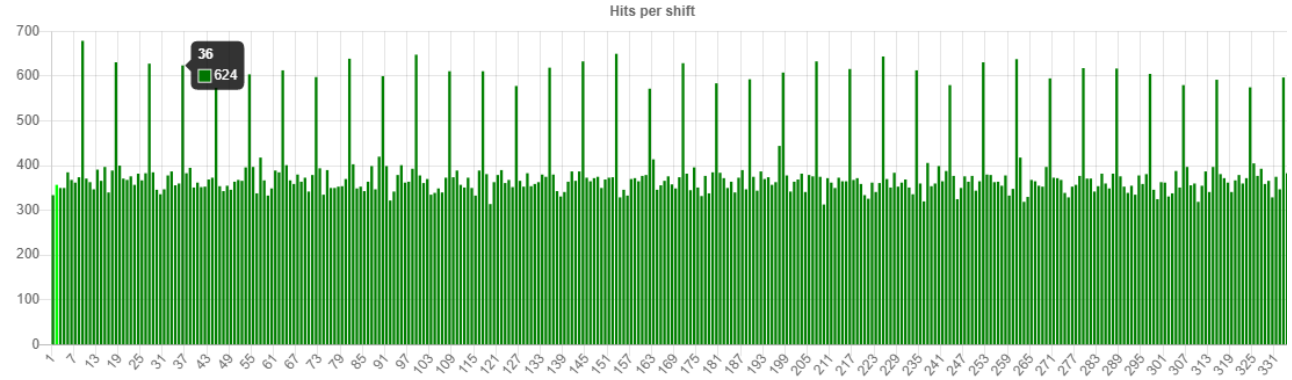
Number of bars: 334

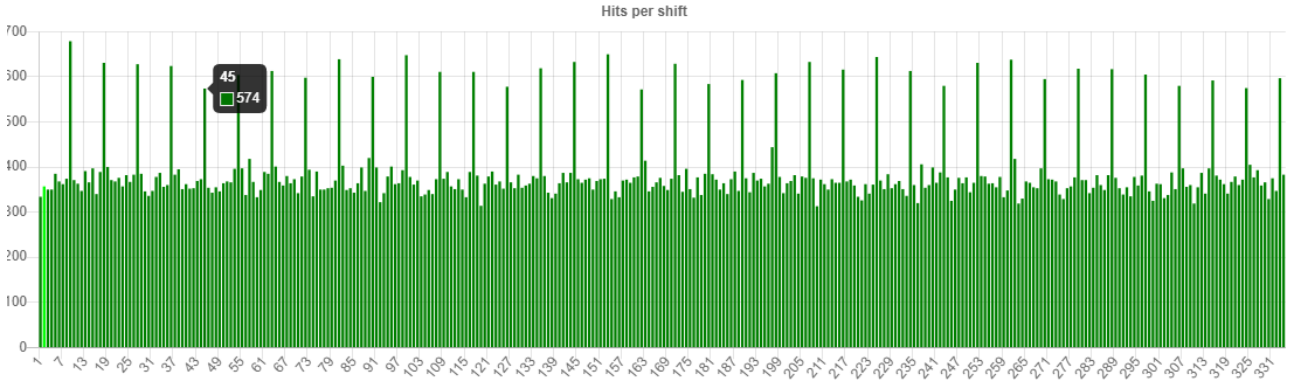


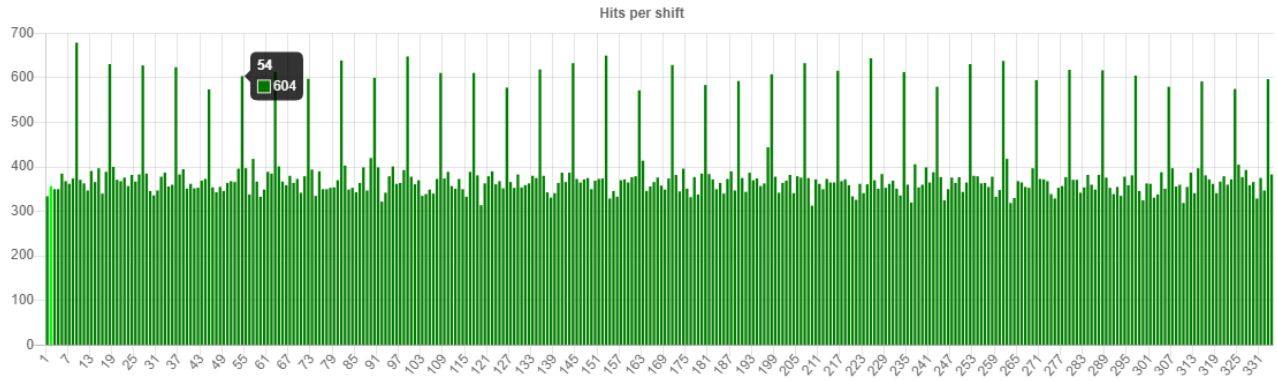



Hits per shift
18
631


Hits per shift
27
628


Hits per shift
36
624


Hits per shift
45
574



Task 7. One-time pad

Answer the following questions related to one-time pad (OTP).

1. Assume that the OTP key is 0101 1100 1101 1011 and the message, encoded as a binary string, is 1100 1000 0110 0111. What is the ciphertext?

	0	1	0	1	1	1	0	0	1	1	0	1	1	0	1	1
⊕	1	1	0	0	1	0	0	0	0	1	1	0	0	1	1	1
	1	0	0	1	0	1	0	0	1	0	1	1	1	1	0	0

2. What is known-plaintext attack?

   This is when an attacker wants to decrypt a cyphertext, the attacker who does not know the key. The attacker may have a copy of two different cipher texts that share the same encryption method.

   This is a method of reverse engineering using a plaintext-ciphertext pair, knowing the encryption algorithm used to resolve the unknown encryption key.

3. Let $n > 1$ be a positive integer. Suppose a careless user used the OTP system to encrypt two n-bit message m_0 and m_1, with the same but unknown n-bit key k and got the corresponding ciphertexts c_0 and c_1. As an attacker, you somehow obtained m_1 and captured c_0, c_1 when they were being transmitted. Explain how you can recover the key k and the other message m_0.

Base formula

$C_0 = k \oplus m_0$

Known	Unknown	Formula
m_1	k	$C_x = k \oplus m_x$
C_0	m_0	
C_1		

$C_1 = k \oplus m_1$

$C_0 = k \oplus m_0$

$m_1 = k \oplus C_1 \therefore C_1 = k + m_1$

$C_1 \oplus m_1 = (k \oplus m_1) \oplus m_1$

$= k \oplus (m_1 \oplus m_1)$

$= k \oplus 0$

$= k$

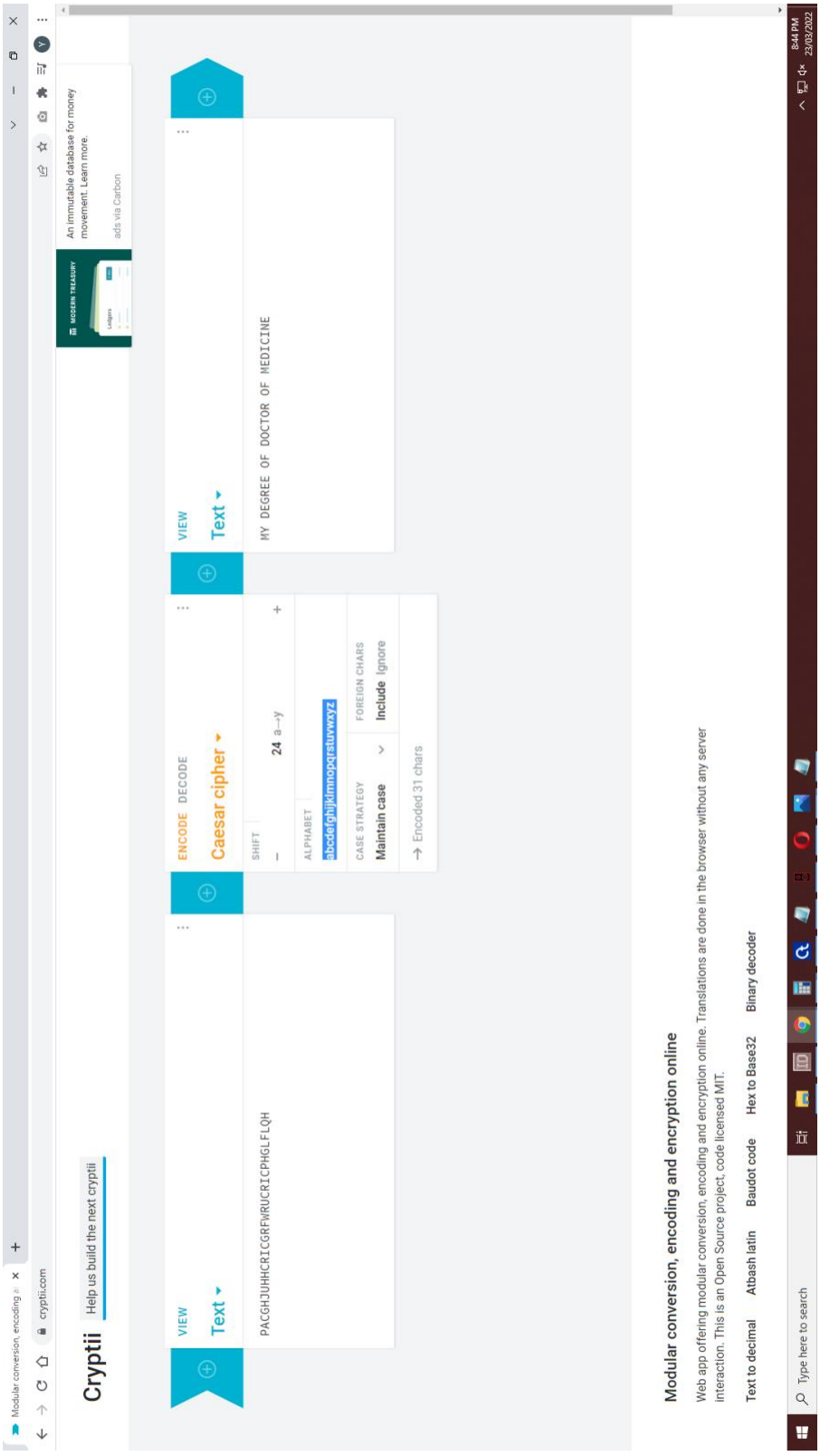
	XOR
0 0	0
0 1	1
1 0	1
1 1	0

XOR on the same values equates to zero

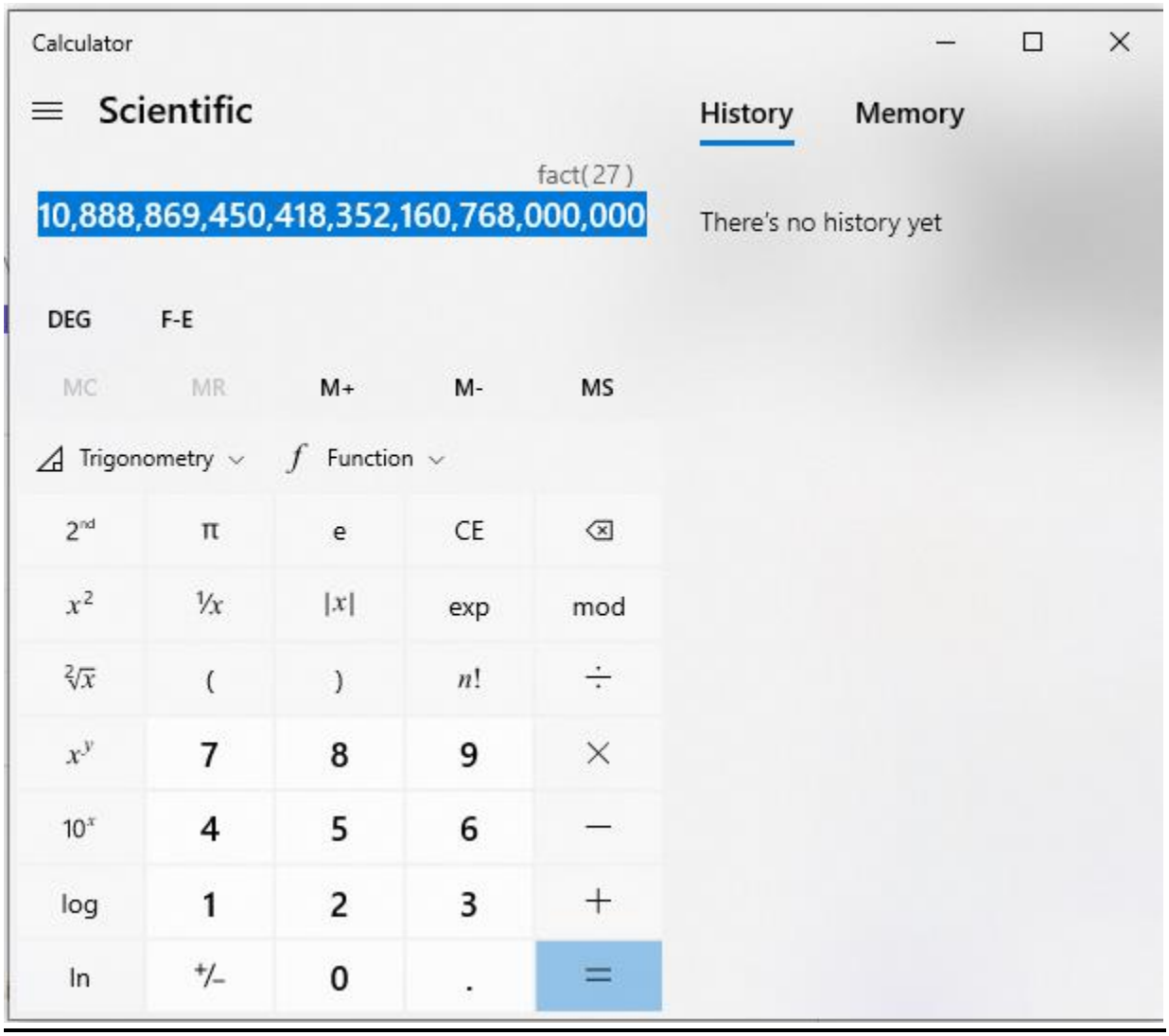
$x \oplus 0 = x$ always

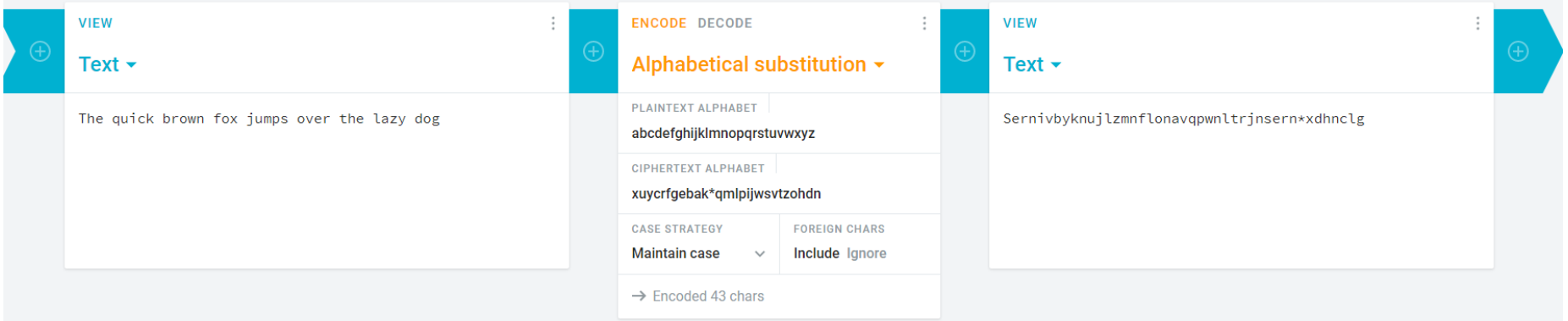
Appendix

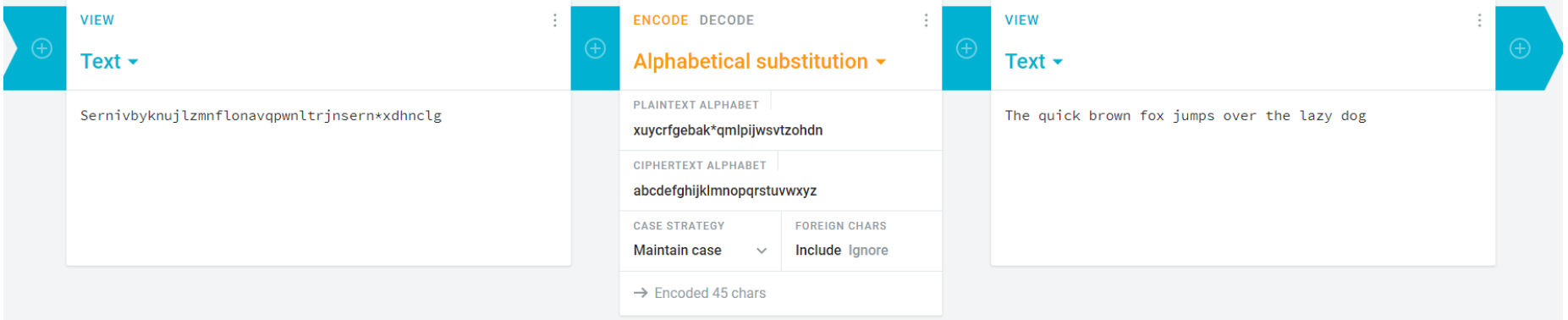
Appendix A



Appendix B


Calculator
Scientific
History
Memory
fact(27)
10,888,869,450,418,352,160,768,000,000
There's no history yet
DEG
F-E
MC
MR
M+
M-
MS
Trigonometry
Function
2nd
π
e
CE
x²
1/x
|x|
exp
mod
∛x
(
)
n!
÷
xʸ
7
8
9
×
10ˣ
4
5
6
−
log
1
2
3
+
ln
+/−
0
.
=


VIEW
Text
The quick brown fox jumps over the lazy dog
ENCODE DECODE
Alphabetical substitution
PLAINTEXT ALPHABET
abcdefghijklmnopqrstuvwxyz
CIPHERTEXT ALPHABET
xuycrfgebak*qmlpijwsvtzohdn
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
Encoded 43 chars
VIEW
Text
Sernivbyknujlzmnflonavqpwnltrjnsern*xdhnclg


VIEW
Text
Sernivbyknujlzmnflonavqpwnltrjnsern*xdhnclg
ENCODE DECODE
Alphabetical substitution
PLAINTEXT ALPHABET
xuycrfgebak*qmlpijwsvtzohdn
CIPHERTEXT ALPHABET
abcdefghijklmnopqrstuvwxyz
CASE STRATEGY
Maintain case
FOREIGN CHARS
Include Ignore
Encoded 45 chars
VIEW
Text
The quick brown fox jumps over the lazy dog