TEXT 1

It is homogeneous text consisting of letter “v” repeated 1500 times.

TEXT 2

Medium diversified text consisting of the phrase “Once You Question Your Own Belief, It's Over

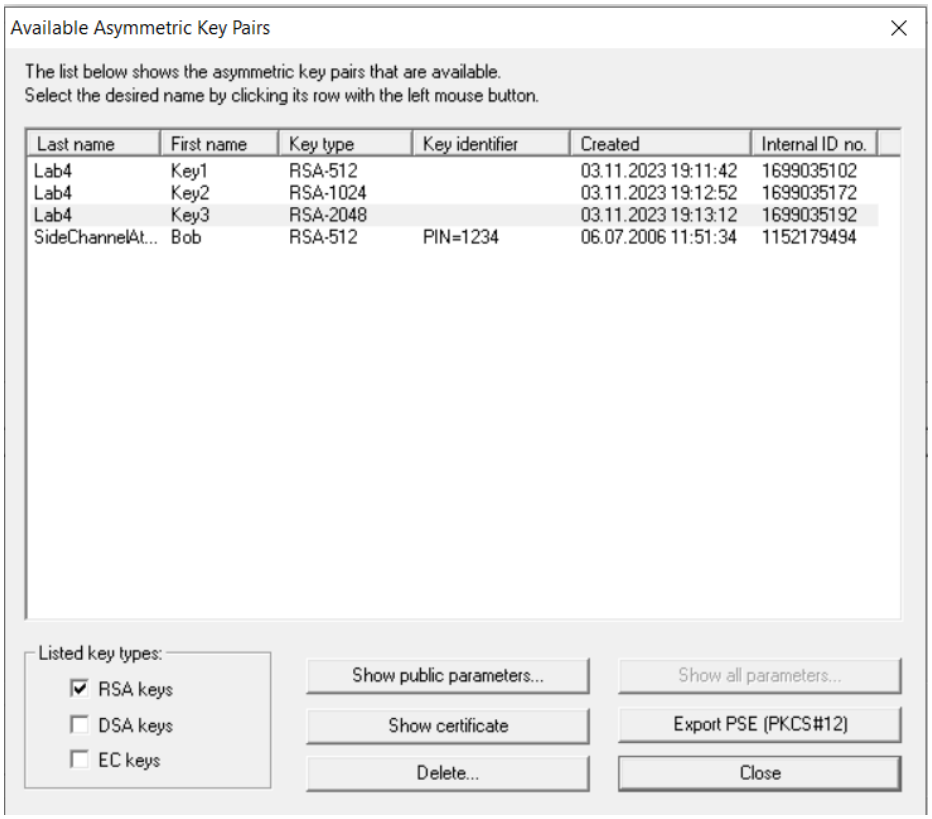
” Repeated 400 times

TEXT 3

Highly diversified text:

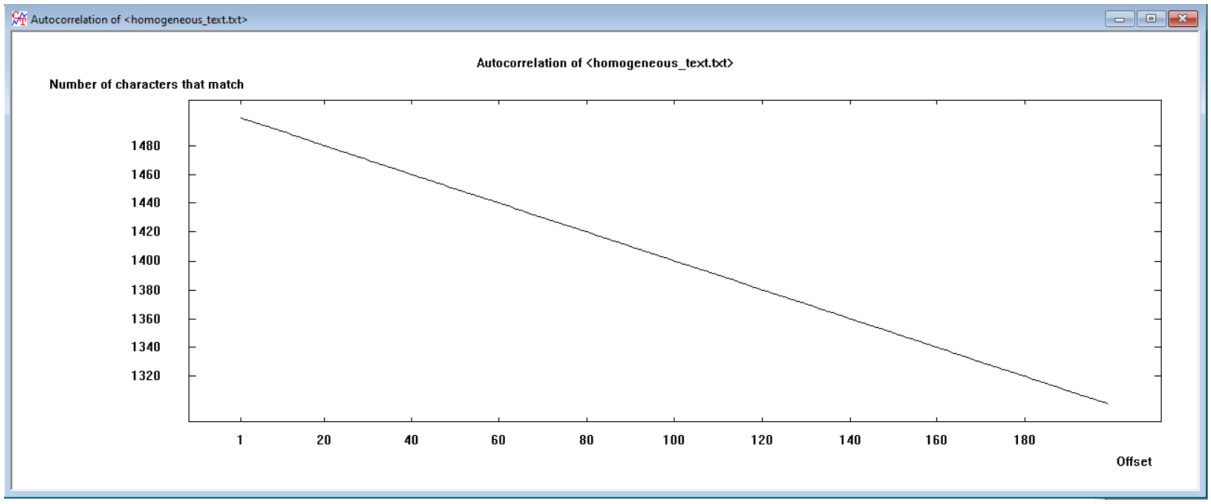
But even if I told you why, I doubt very strongly that the knowledge would change anything at all but let's just say that I take the time to explain it to you. What do you think would happen then? My goal is to fulfill the dream even Jiraya sensei was unable to achieve that is to create peace and bring about justice. Oh I see that is noble of you that would be justice. However what about my family? My friends, my village they suffered the same fate as this village at the hands of you hidden leaf ninja. How's it fair to let only you people preach about peace and justice once the land of fire and the hidden leaf had grown too big to protect the national interests. They forced feudal clans to wage war against each other and profited from it otherwise the people of the villages would've starved as it happened our little nation and its villages became the battlefield where the great nations waged through war each time they did our nation was ravaged and laid to waste after many such battles the great nations stabilized but our smaller nation suffered and barely recovered. You and I are both seeking the very same thing we both want to achieve the peace that jiraya sensei envisioned, you and I are the same, we’re both motivated by our desire for peace and justice. The justice that I have delivered against the leaf village is no different from what you are trying to do to me. Everyone feels the same pain in losing something dear, you and I both have experience that same pain. You strive for your justice and I strive for mine we’re both just ordinary men who have been driven to seek vengeance in the name of justice and if comes call vengeance justice such justice will only breed further vengeance and trigger a vicious cycle of hatred, right now we live in such a cycle. I know the past and can foretell our future it is the same as our history so we believe that Human beings simply cannot understand each other and they never will that the shinobi world is ruled by hatred and hatred alone. So naruto how would u confront this hatred in order to create peace? I want to know what your answer…..

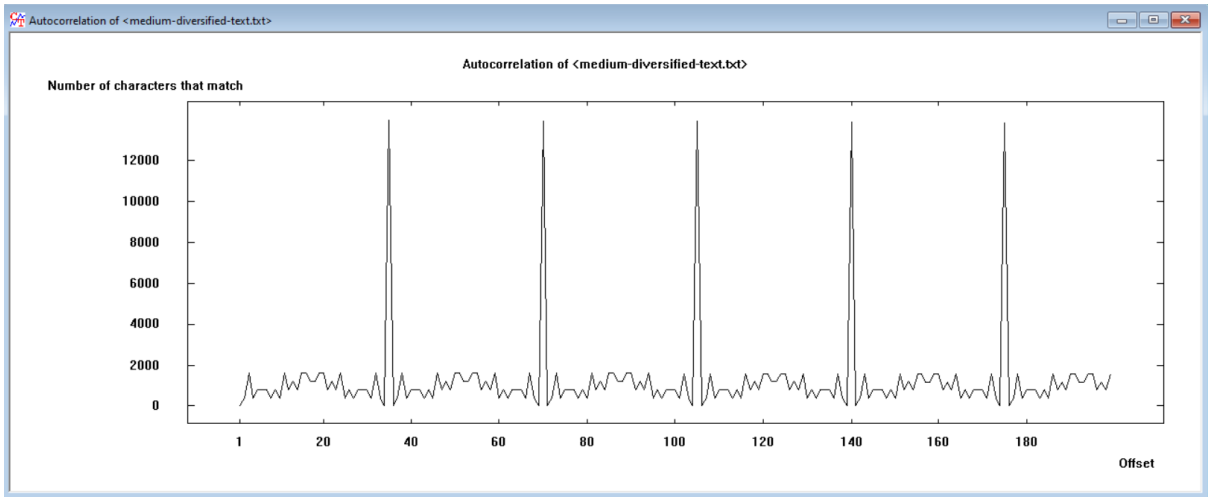
TASK 1.2

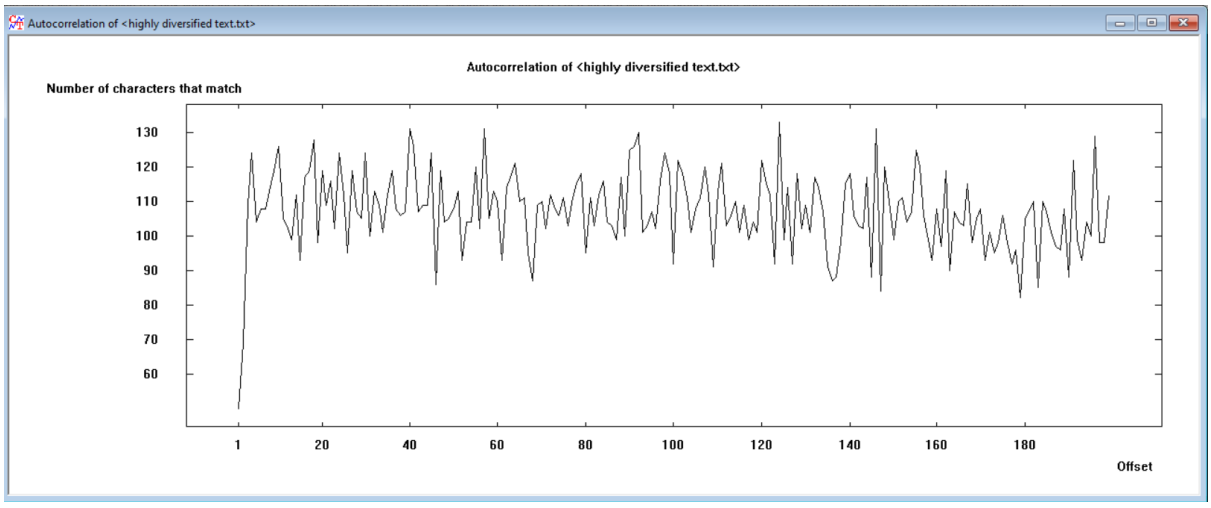


Entropy of plaintext and ciphertext depending on key length				
	Plaintext	Ciphertext		
Key length(bits)	-	512	1024	2048
homogeneous	0	5.98/8	6.78/8	7.41/8
middle-diversified	3.71/4.7	7.93/8	7.96/8	7.98/8
highly diversified	4.17/4.7	7.92/8	7.9/8	7.9/8

Autocorrelation of plaintext:

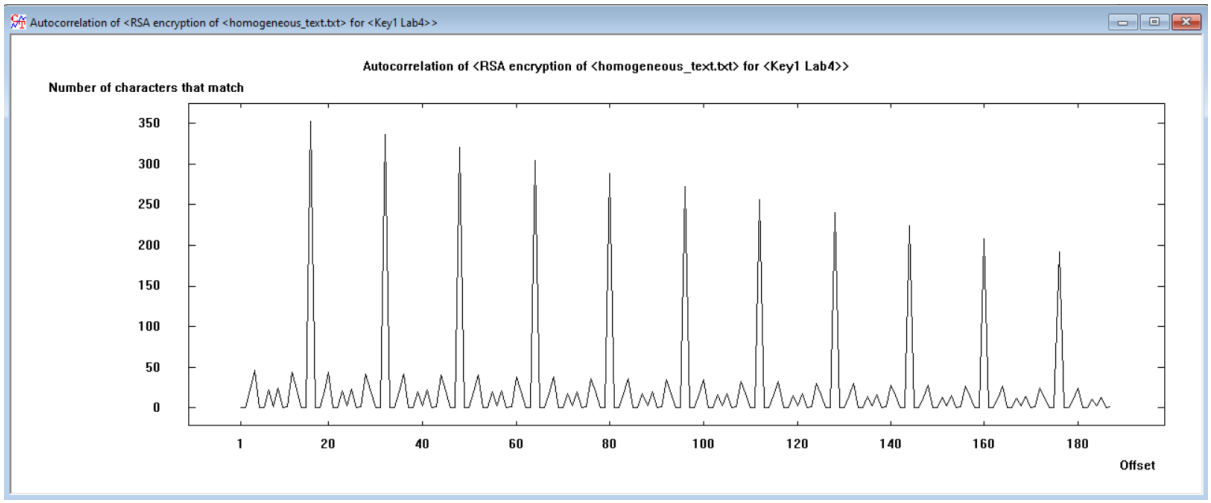




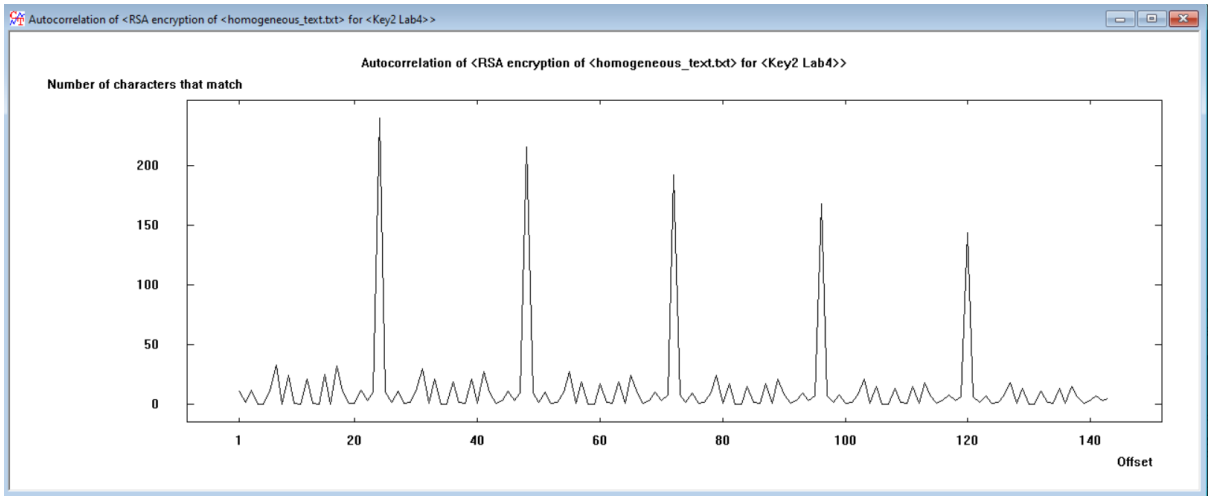


Ciphertext(homogeneous text) autocorrelation

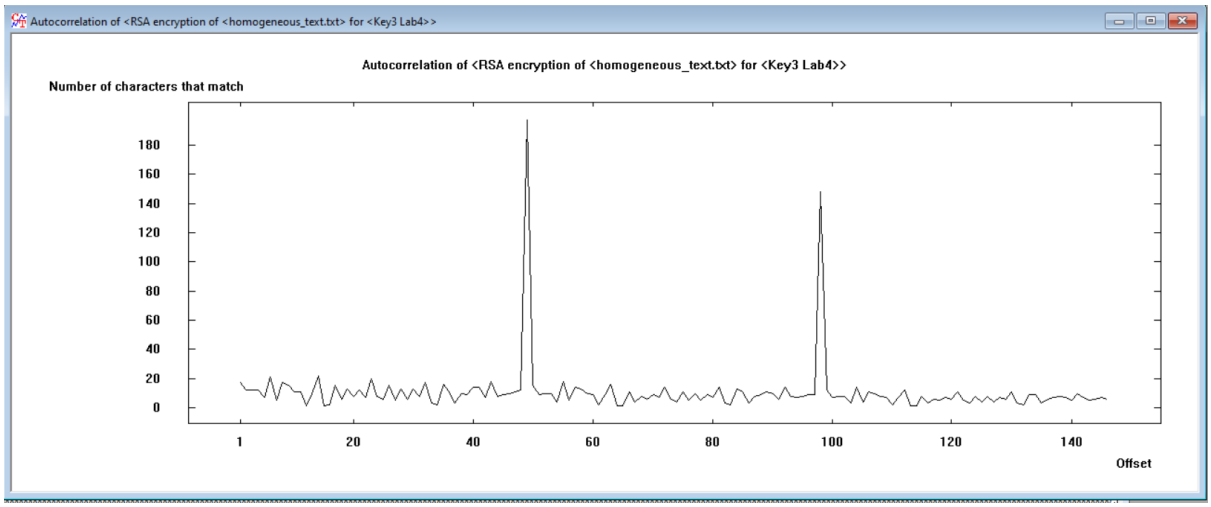
512:



1024:

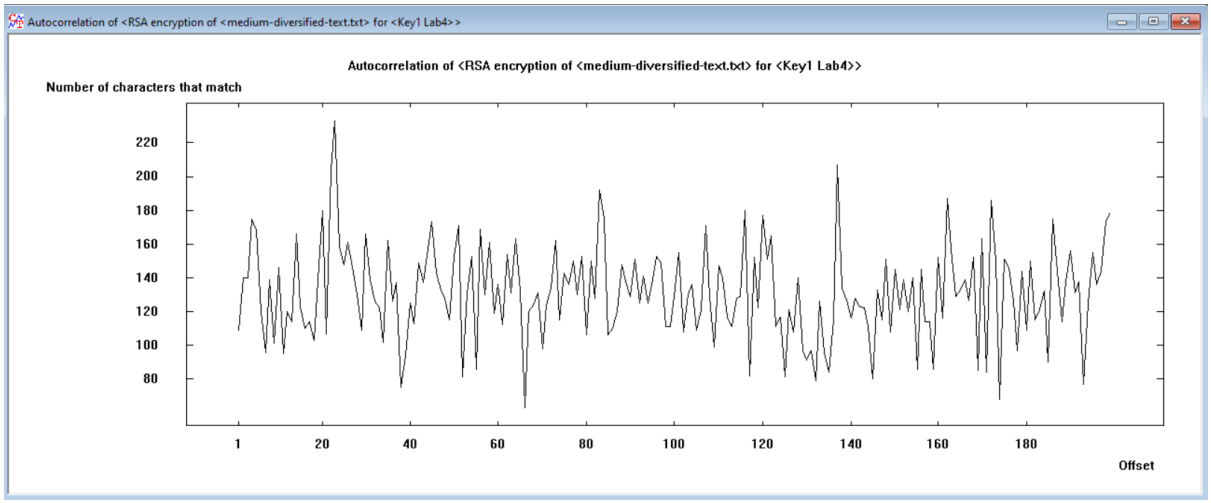


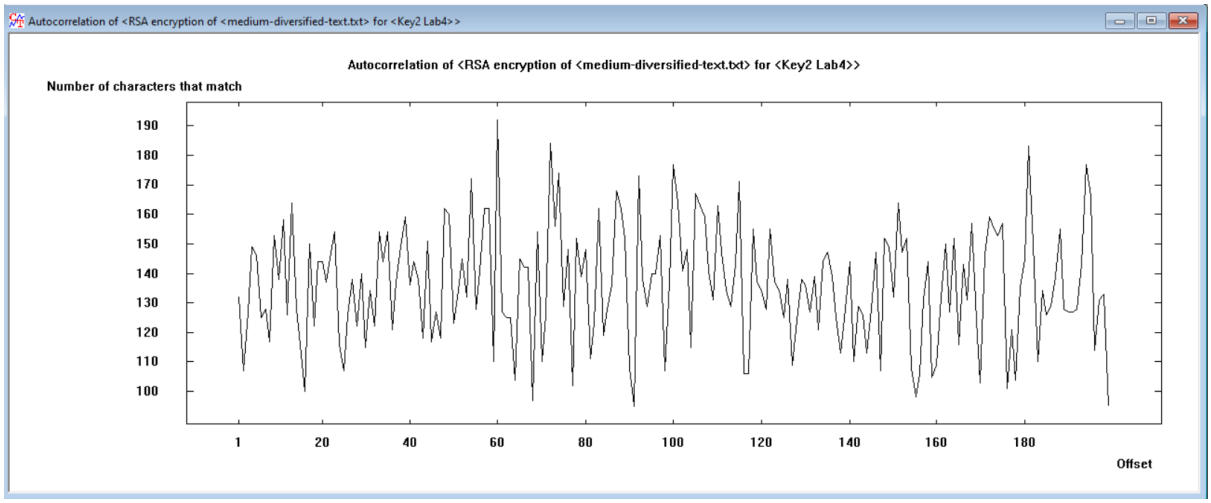
2048:

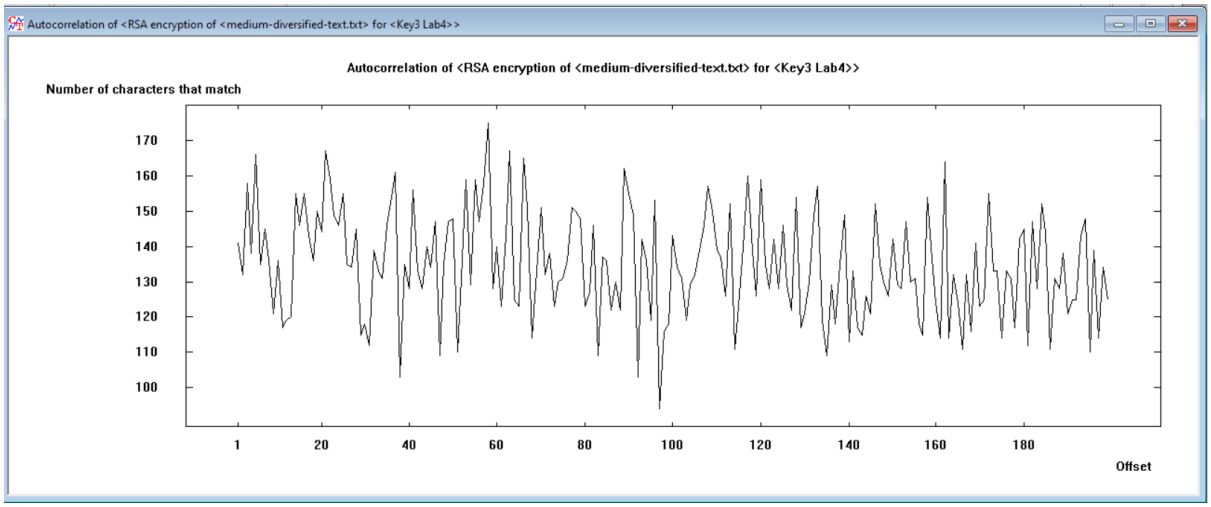


Ciphertext(middle diversified text) autocorrelation:

512:

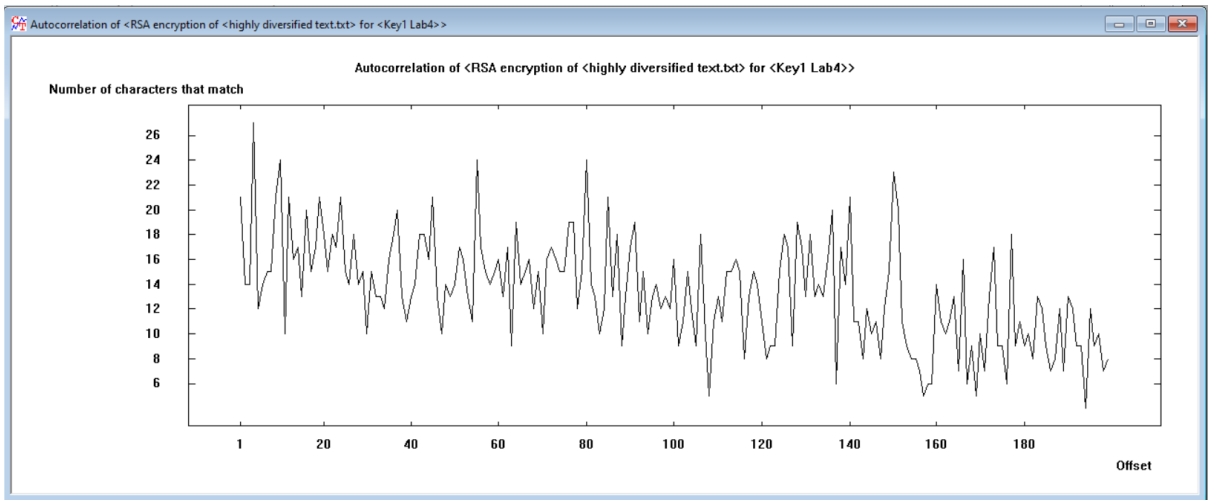




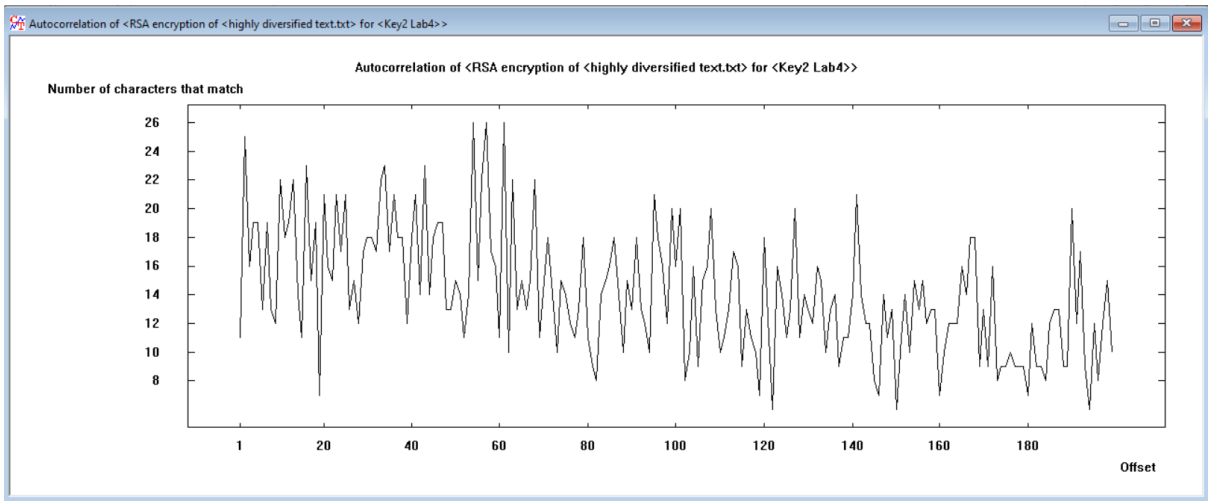


Ciphertext(highly diversified text) autocorrelation:

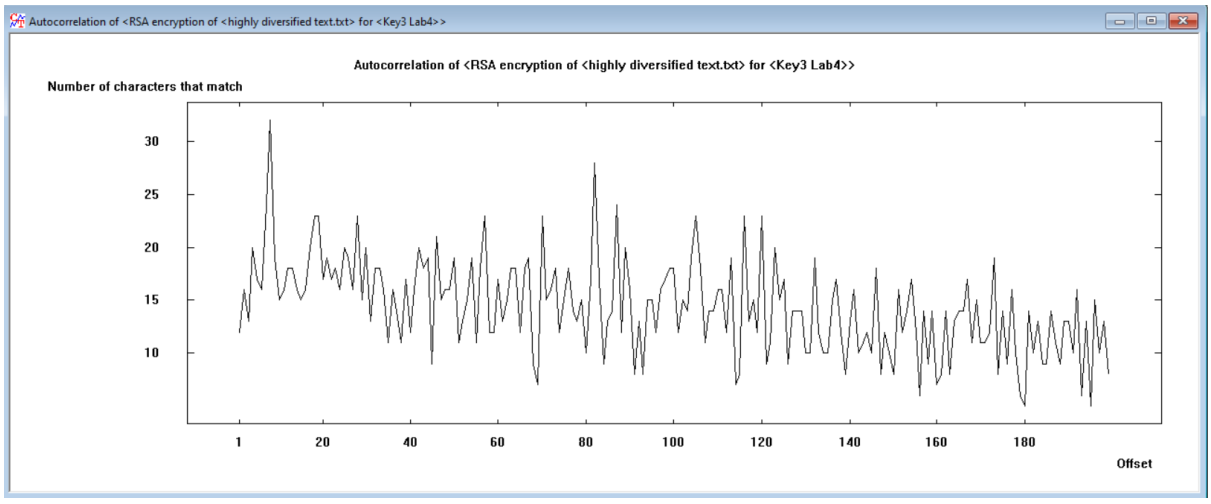
512:



1024:



2048:

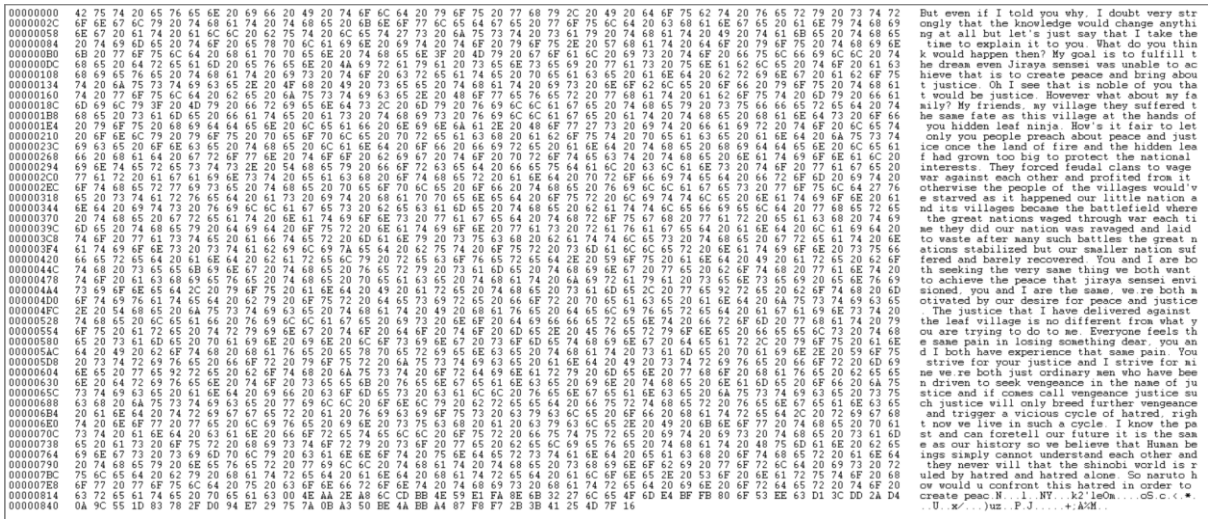


Time of encryption and decryption for different files						
	Encryption			Decryption		
key length	512	1024	2048	512	1024	2048
1 mb file	0.28	0.424	0.794	3.726	9.673	33.183
2mb file	0.549	0.872	1.572	7.388	19.343	66.066
5mb file	1.381	2.13	3.922	18.515	48.273	165.567

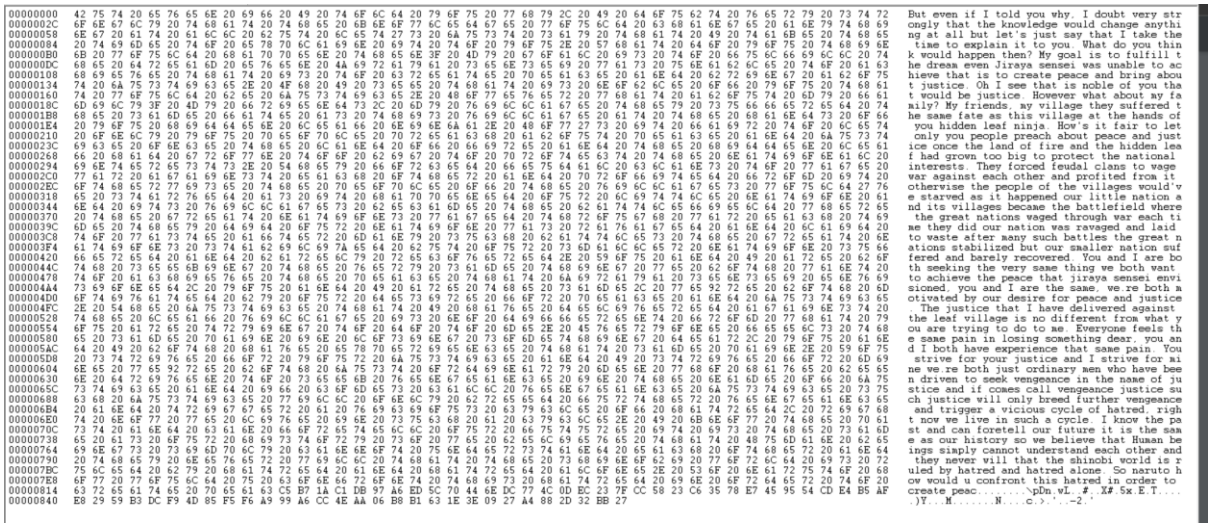
Time of encryption and decryption using AES for different files						
	Encrpytion			Decryption		
key length	128	192	256	128	192	256
1 mb file	<0.3	<0.3	<0.3	<0.3	<0.3	<0.3
2mb file	<0.5	<0.5	<0.5	<0.5	<0.6	<0.7
5mb file	<0.6	<0.6	<0.6	<0.6	<0.7	<1

RSA 512:

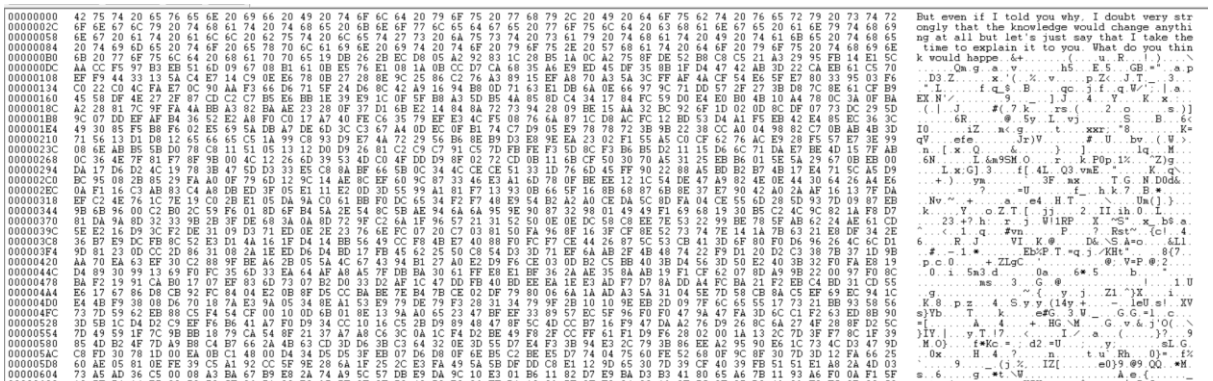
Change the value of one byte(last byte):



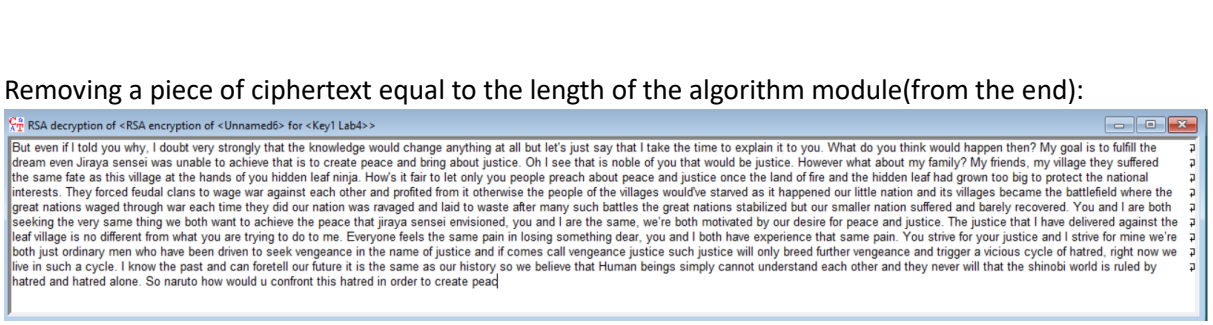
Removing one byte:



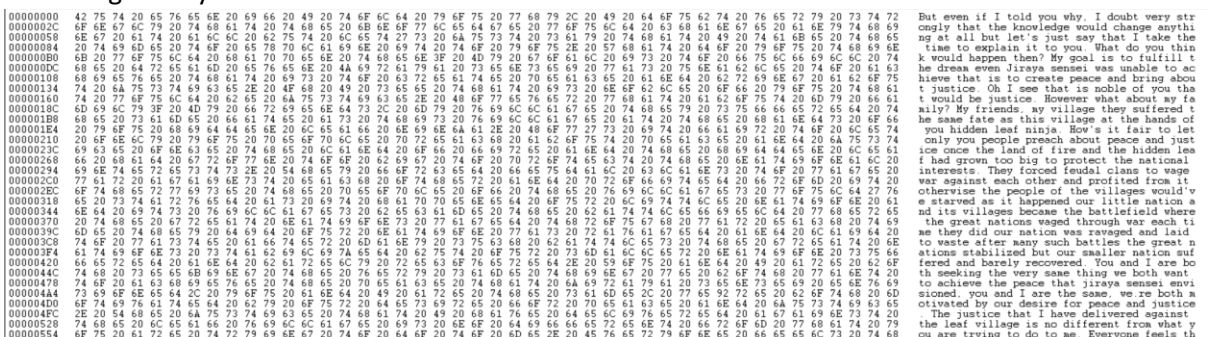
Removing several bytes:



Removing a piece of ciphertext equal to the length of the algorithm module(from the end):

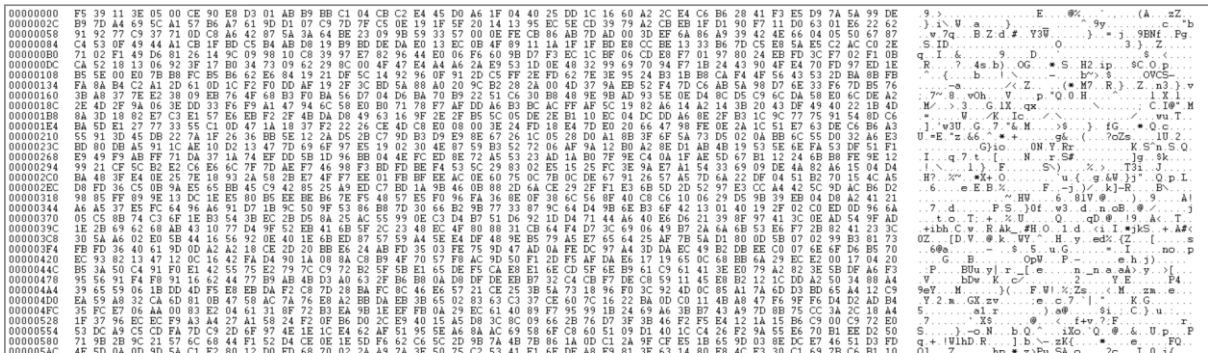


RSA 1024:

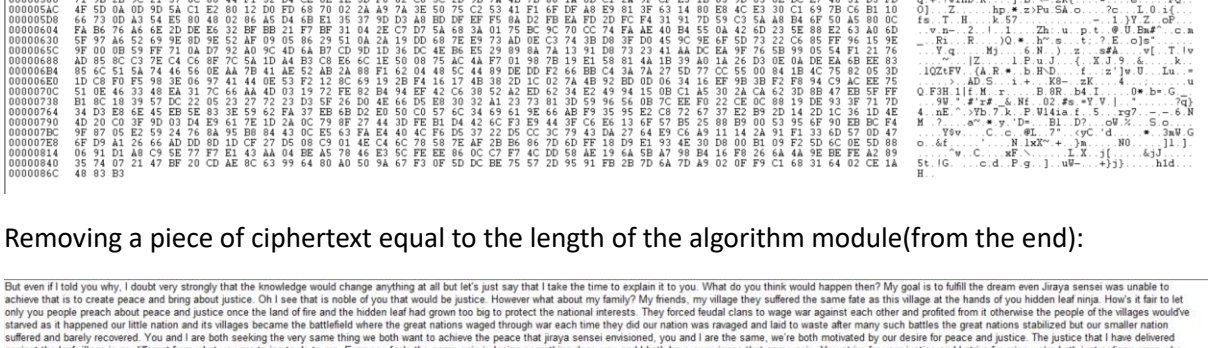


Removing one byte:

Removing several bytes:



Removing a piece of ciphertext equal to the length of the algorithm module(from the end):



TASK 1.7

The key length significantly influences the entropy of encrypted text primarily when dealing with homogeneous text. It's evident that as the key length increases, the entropy of the encrypted text also rises. However, when working with highly diverse and middle-diversified text, the key length does not seem to have any noticeable effect on the post-encryption text's entropy.

TASK 1.8

When dealing with homogeneous and middle diversified text, there is a trend: longer keys lead to wider gaps between the "peaks" in the graphs. However, with highly diverse text, the key length doesn't seem to make any difference. The autocorrelation graphs look pretty much the same, without any clear recurring patterns.

TASK 1.9

In the context of the examined algorithm, the entropy of the encrypted text consistently surpasses that of the original text, without regard to the text's characteristics or the key length. When dealing with less varied texts, the encrypted text's entropy might occasionally fall slightly short of the maximum value, but for more diverse texts, it consistently approaches the maximum attainable entropy.

TASK 1.10

The time it takes for encryption goes up as the file size and key length increase. But for files up to 5MB, it never took more than 4 seconds, which was quite manageable.

Decrypting files always to ok a lot more time than encrypting them, especially when dealing with bigger files and longer encryption keys. With a 2048-bit key, decryption consistently took more than 30 seconds, and for a 5 MB file, it often dragged on for over 2.5 minutes.

TASK 1.11

The encryption process for symmetric algorithms typically lasted around 0.3 seconds. It can be concluded that symmetric algorithm encryption happens virtually instantly. There was no noticeable difference with larger file sizes or longer keys.

Decryption, however, required more time as file sizes and key lengths grew. For smaller files (up to 2 MB), decryption finished in less than a second, possibly even in under 0.7 seconds. Even for a 5 MB file, decryption took nearly a full second. This slight increase in time might have been affected by other concurrent system processes, but it didn't pose a significant inconvenience.

TASK 1.12

If you modify a single byte, only a segment of the text changes after decryption, with the altered byte spanning the length of the block used in the algorithm (either 512 bits or 1024 bits). The rest of the text remains unchanged.

When a single byte is removed, the text alteration starts from the block where the byte was deleted, extending to the very end of the text and encompassing the key's length. Deleting multiple bytes yields a similar outcome as removing a single byte: information is lost from the block with the first deleted byte to the end of the text, regardless of the locations of the other deleted bytes. Deleting bytes from the beginning of the text results in the complete loss of the entire content.

If you eliminate a fragment from the ciphertext that matches the block length of the algorithm, only a segment of the same length in the text is lost. The information before and after the deleted block remains intact.

TASK 1.13

Certainly, the segment to be removed must align with the algorithm block's length or multiples of it. In this case, only the portion of the text matching the length of the deleted block is affected, while the remainder of the text remains legible after decryption.

TASK 1.14

Asymmetric algorithms provide greater security compared to symmetric algorithms due to the use of different keys for encryption and decryption. In symmetric algorithms, a single key is employed for both tasks, which means that if one key is compromised, the entire message can be decrypted easily. In contrast, asymmetric algorithms use distinct keys, so knowing one key does not guarantee the ability to decrypt the message, thus enhancing security. Regarding the entropy of the plaintext and encrypted data, both types of algorithms perform similarly, exhibiting better performance with dissimilar texts as opposed to homogeneous ones, regardless of key length.

However, when it comes to the speed of encryption and decryption operations, symmetric algorithms excel. Their encryption and decryption processes are considerably faster due to shorter key lengths and less complex mathematical operations. Asymmetric algorithms, on the other hand, exhibit significantly longer decryption times, particularly for files larger than 5 MB, often surpassing 2.5 minutes. This makes them impractical for encrypting large data files. Furthermore, asymmetric algorithms are more prone to data misrepresentation or partial loss in messages, often resulting in a significant portion of the plaintext or even the entire text being lost. In contrast, symmetric algorithms, depending on the mode of operation, may only lose a very small portion of the text or even just 1 byte.

TASK 1.15

If our priority is to swiftly encrypt and decrypt large volumes of data in near real-time, symmetric algorithms are the more suitable choice, as they involve less complex mathematical operations. Similarly, if we anticipate frequent interference in the ciphertexts, symmetric algorithms will result in a significantly smaller portion of the text being affected. On the contrary, if the data to be encrypted is relatively small, interference is minimal, and our primary concern is enhancing security rather than the speed of encryption and decryption, then asymmetric algorithms can be employed.