Assignment on Computer Data and Network Security

Task-1

Submitted by: Submitted To:

Md. Wasif Mustahid [**Quazi Ishtiaque Mahmud Rafi**](https://www.facebook.com/profile.php?id=100000932155407&ref=br_rs)

Reg: 2016831031 Lecturer

Dept of Software Engineering Sust

Introduction

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Encryption is widely used on the internet to protect user information being sent between a browser and a server, including passwords, payment information and other personal information that should be considered private. Organizations and individuals also commonly use encryption to protect sensitive data stored on computers, servers and mobile devices like phones or tablets.

How encryption works

Unencrypted data, often referred to as [plaintext](http://searchsecurity.techtarget.com/definition/plaintext), is encrypted using an encryption [algorithm](http://whatis.techtarget.com/definition/algorithm) and an encryption [key](http://searchsecurity.techtarget.com/definition/key). This process generates [ciphertext](http://whatis.techtarget.com/definition/ciphertext) that can only be viewed in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following the same steps but reversing the order in which the keys are applied. Today's most widely used encryption algorithms fall into two categories: symmetric and asymmetric.

[Symmetric-key](http://searchsecurity.techtarget.com/definition/secret-key-algorithm) ciphers, also referred to as "secret key," use a single key, sometimes referred to as a shared secret because the system doing the encryption must share it with any entity it intends to be able to decrypt the encrypted data. The most widely used symmetric-key cipher is the Advanced Encryption Standard ([AES](http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard)), which was designed to protect government classified information.

Symmetric-key encryption is usually much faster than asymmetric encryption, but the sender must exchange the key used to encrypt the data with the recipient before the recipient can perform decryption on the ciphertext. The need to securely distribute and manage large numbers of keys means most cryptographic processes use a symmetric algorithm to efficiently encrypt data, but they use an asymmetric algorithm to securely exchange the secret key.

[Asymmetric cryptography](http://searchsecurity.techtarget.com/definition/asymmetric-cryptography), also known as public key cryptography, uses two different but mathematically linked keys, one [public](http://searchsecurity.techtarget.com/definition/public-key) and one [private](http://searchsecurity.techtarget.com/definition/private-key). The public key can be shared with everyone, whereas the private key must be kept secret. The [RSA encryption algorithm](https://searchsecurity.techtarget.com/definition/RSA) is the most widely used public key algorithm, partly because both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute provides a method of assuring not only confidentiality, but also the integrity, authenticity and nonreputability of electronic communications and data at rest through the use of [digital signatures](http://searchsecurity.techtarget.com/definition/digital-signature).

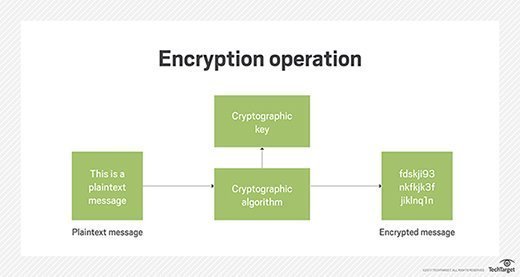


Figure: Encryption Process

Definitions and Abbreviation’s:

|  |  |
| --- | --- |
| Encryption | the process of converting information or data into a code, especially to prevent unauthorized access. |
| Decryption | **Decryption** is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. |
| Encryption key | An **encryption key** is a random string of bits created explicitly for scrambling and unscrambling data |
| Decryption key | **Decryption key** is the code that you need to transform an encrypted message, document, or other data into a form that can be freely read |
| Cipher | In cryptography, a **cipher** (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure |
| Substitution cipher | Substitution Cipher A substitution cipher is a type of encryption where characters or units of text are replaced by others in order to encrypt a text sequence. |
|  |  |
|  |  |

A Encrypt message to Decrypt Procedure:

Encrypted Paragraph:

aceah toz puvg vcdl omj puvg yudqecov, omj loj auum klu thmjuv hs klu zlcvu shv zcbkg guovz, upuv zcmdu lcz vuwovroaeu jczoyyuovomdu omj qmubyudkuj vukqvm. klu vcdluz lu loj avhqnlk aodr svhw lcz kvopuez loj mht audhwu o ehdoe eunumj, omj ck toz yhyqeoveg auecupuj, tlokupuv klu hej sher wcnlk zog, klok klu lcee ok aon umj toz sqee hs kqmmuez zkqssuj tckl kvuozqvu. omj cs klok toz mhk umhqnl shv sowu, kluvu toz oezh lcz yvhehmnuj pcnhqv kh wovpue ok. kcwu thvu hm, aqk ck zuuwuj kh lopu eckkeu ussudk hm wv. aonncmz. ok mcmukg lu toz wqdl klu zowu oz ok scskg. ok mcmukg-mcmu klug aunom kh doee lcw tuee-yvuzuvpuj; aqk qmdlomnuj thqej lopu auum muovuv klu wovr. kluvu tuvu zhwu klok zlhhr klucv luojz omj klhqnlk klcz toz khh wqdl hs o nhhj klcmn; ck zuuwuj qmsocv klok omghmu zlhqej yhzzuzz (oyyovumkeg) yuvyukqoe ghqkl oz tuee oz (vuyqkujeg) cmubloqzkcaeu tuoekl. ck tcee lopu kh au yocj shv, klug zocj. ck czm’k mokqvoe, omj kvhqaeu tcee dhwu hs ck! aqk zh sov kvhqaeu loj mhk dhwu; omj oz wv. aonncmz toz numuvhqz tckl lcz whmug, whzk yuhyeu tuvu tceecmn kh shvncpu lcw lcz hjjckcuz omj lcz nhhj shvkqmu. lu vuwocmuj hm pczckcmn kuvwz tckl lcz vueokcpuz (ubduyk, hs dhqvzu, klu zodrpceeuaonncmzuz), omj lu loj womg juphkuj ojwcvuvz owhmn klu lhaackz hs yhhv omj qmcwyhvkomk sowcecuz. aqk lu loj mh dehzu svcumjz, qmkce zhwu hs lcz ghqmnuv dhqzcmz aunom kh nvht qy. klu uejuzk hs kluzu, omj aceah’z sophqvcku, toz ghqmn svhjh aonncmz. tlum aceah toz mcmukgmcmu lu ojhykuj svhjh oz lcz lucv, omj avhqnlk lcw kh ecpu ok aon umj; omj klu lhyuz hs klu zodrpceeu- aonncmzuz tuvu scmoeeg jozluj. aceah omj svhjh loyyumuj kh lopu klu zowu acvkljog, zuykuwauv 22mj. ghq loj aukkuv dhwu omj ecpu luvu, svhjh wg eoj, zocj aceah hmu jog; omj klum tu dom dueuavoku hqv acvkljog-yovkcuz dhwshvkoaeg khnukluv. ok klok kcwu svhjh toz zkcee cm lcz ktuumz, oz klu lhaackz doeeuj klu cvvuzyhmzcaeu ktumkcuz auktuum dlcejlhhj omj dhwcmn hs onu ok klcvkg-klvuu

Description of process:

We will use Substitution cipher to do this. It is known that or observe that the frequency distribution of English word is given bellow:

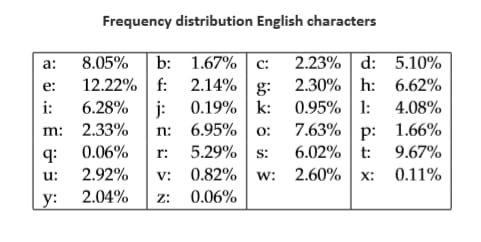


Figure : d

Also frequent word are given bellow:

Frequent One Letter words:

’a’, ’i’

Frequent Two Letter words:

’of’, ’to’, ’in’, ’it’, ’is’, ’be’, ’as’, ’at’, ’so’, ’we’, ’he’, ’by’, ’or’, ’on’, ’do’, ’if’, ’me’, ’my’, ’up’, ’an’, ’go’, ’no’, ’us’, ’am’

Frequent Three Letter words:

’the’, ’and’, ’for’, ’are’, ’but’, ’not’, ’you’, ’all’, ’any’, ’can’, ’had’, ’her’, ’was’, ’one’, ’our’, ’out’, ’day’, ’get’, ’has’, ’him’, ’his’, ’how’, ’new’, ’now’, ’old’, ’see’, ’two’, ’way’, ’who’, ’boy’, ’did’, ’let’, ’put’, ’say’, ’she’, ’too’

By analyzing the decrypted message and using Hadoop map reduce distributed system for word count or github code in the link :

o : 2 hs:10 qy:1

au : 1 kh:8 tu:1

ck : 6 lu:6 wg:1

cm : 1 mh:1 wv:2

cs : 1 ok:8 zh:1

hm : 3 oz:6

aon : 2 aqk : 4 dom : 1

eoj : 1 ghq : 1 hej : 1

hmu : 1 hqv : 1 khh : 1

klu : 15 lcw : 3 lcz : 10

loj : 7 mhk : 2 mht : 1

omj : 18 onu : 1 shv : 3 sov : 1 toz : 11 umj : 1 zog : 1

Substituting the Letters:

First step:

Here we can find there are o in the middle of the text.so ’o’ can be ‘a/I’0. but usually ’ I’ doesn’t sit in middle of simple sentence .even if ‘I’ sits in the middle, then the sentence will be complex or com- pound. So ‘o=a’

Second Step:

From the analysis the highest frequency that is 10 of two length word is ’hs’.Now comparing with section most frequent word of two length is ’of’.

h = o , s = f

Next higher frequency word is ’kh’.We know that h = o, so from we can say that ’k’ is mapped to ’t’ k = t Another two length word is ’ck’ whose frequency is 6.We know that k = t, a two-length word that ends with ’t’ either can be ’it’ or ’at’

.Since ’a’ is mapped with ’o’, c = i c = i

Third Step:

Most frequent three length word in the encrypted text is ’omj’ whose frequency is 18. We already know that o = a, hence Most frequent three length word that starts with ’a’ is ’and’. m = n ,j = d

Second most frequent three length word is ’klu’ and its frequency is 15.Since we already mapped ’k’ to ’t’ and ’u’ to ’e’ so the three length word that starts with ’t’ and ends with ’e’ is ’the’. l = h

Another three length word is ’aqk’. We already know the value of ’k’ which is ’t’.So we can guess the word is ’but’. a = b ,q = u Again if we take another three length word ’hej’, since we already know the value of ’h’ and ’j’. So, a three length word that starts with ’o’ and ends with ’d’ can be found which is ’old’ e = l Now the first word ’aceah’ of the encrypted text can be decrypted from these values. In this way we can decrypt the text. aceah = bi?bo (12) By google search we find that, e = l (13) So, the final first word, aceah = bilbo (14) In this way, now we can find all the words.

Code :

The code is given bellow in github link:

<https://github.com/wasif31/Computer-data-and-network-security>

Decrypted Message:

bilbo was very rich and very peculiar, and had been the wonder of the shire for sixty years, ever since his remarkable disappearance and unexpected return. the riches he had brought back from his travels had now become a local legend, and it was popularly believed, whatever the old folk might say, that the hill at bag end was full of tunnels stuffed with treasure. and if that was not enough for fame, there was also his prolonged vigour to marvel at. time wore on, but it seemed to have little effect on mr. baggins. at ninety he was much the same as at fifty. at ninety-nine they began to call him well-preserved; but unchanged would have been nearer the mark. there were some that shook their heads and thought this was too much of a good thing; it seemed unfair that anyone should possess (apparently) perpetual youth as well as (reputedly) inexhaustible wealth. it will have to be paid for, they said. it isn’t natural, and trouble will come of it! but so 2 far trouble had not come; and as mr. baggins was generous with his money, most people were willing to forgive him his oddities and his good fortune. he remained on visiting terms with his relatives (except, of course, the sackvillebagginses), and he had many devoted admirers among the hobbits of poor and unimportant families. but he had no close friends, until some of his younger cousins began to grow up. the eldest of these, and bilbo’s favourite, was young frodo baggins. when bilbo was ninety-nine he adopted frodo as his heir, and brought him to live at bag end; and the hopes of the sackville- bagginses were finally dashed. bilbo and frodo happened to have the same birthday, september 22nd. you had better come and live here, frodo my lad, said bilbo one day; and then we can celebrate our birthday-parties comfortably together. at that time frodo was still in his tweens, as the hobbits called the irresponsible twenties between childhood and coming of age at thirty-three