CP3404 Information Security Assignment

Cheng Peng 10.18.2018

Student Number: JC44403

Information Security: A Report on Security and Certification Jobs, Authentication Methods and Cryptanalysis of Substitution Ciphers

Abstract:

Information Security issues nowadays has become the necessary and urgent problem to be solved during the information revolution era. Consequently, to command the necessary skill and information security related concepts is quite of significance. The report is aimed to help with raising the awareness of information security in the reality use, problem solving, and critical thinking improvement. Author will use google search engine to find best matched answer on the Google Scholar or related Scientific website to solve Job Availability, Security Policy, Authentication, Encryption and Decryption problems. The paper will be directed into 5 sections. In the first section, the author will list a table of available job positions that require security and certification as well as their related introductions to assist you take knowledge of job offered on the market. In the second section, author will tell you what is One Time Pad (OTP) and its application today. The author will lead you to have a trial on using OTP as well. Then in the third part, the author will create a BYOD policy for JCU based on two different organization’s BYOD Policy. Forth part follows with introduction to Open Authentication (OAuth) as well as its pros and cons. Finally, in the fifth part, the author will decrypt lines of code which encrypted with Substitution Cipher using English letter Frequency Comparison method.

Part 1 Security and Certification Jobs

Introduction:

It is of significance for IT guys to find a proper job related to certification and security if you are interested in information security after graduation. The table below will list most popular jobs related to security and certification. More information such as employer, job title, description of the job and salary range will be offered as reference to assist you find a good job related to information security.

Security and Certification Jobs Table:

|  |  |  |  |
| --- | --- | --- | --- |
| employer | job title | description of the job | Salary range |
| General Dynamics Information Technology Inc. etc. (Payscale, 2018) | Systems Administrator | Systems administrators are responsible for ensuring their organization's computer systems are well maintained and operate reliably. | $42,531 - $85,813 |
| Cisco Systems Inc. etc. (PayScale, 2018) | Network Engineer | Network engineers work around their employers' computer network designs and maintenance. They paid by solarized not by paid in hours. | $46,849 - $102,602 |
| Science Applications International Corporation  (Payscale, CompTIA Security+ Salary | PayScale, 2018) | Information Security Analyst | Information security analysts takes responsible to provide security solutions and problem solving service for their companies. | $50,117 - $104,032 |
| Hewlett-Packard Company  Etc. (PayScale, 2018) | Information Technology (IT) Manager | An information technology (IT) manager supervises their company's computer infrastructure and related areas of concern. | $51,008 - $128,850 |
| General Dynamics Information Technology Inc  (Average Information Technology (IT) Manager Salary, 2018) | Network Administrator | Network administrators take responsibility for the upkeep of computer software and hardware maintenance as well as system. | $40,272 - $79,657 |
| The PNC Financial Services Group, Inc. (PayScale, 2018) | Information Technology Specialist | Information technology specialists work closely with a variety of technology products, from their design to regular repair and upkeep. | $35,515 - $95,571 |
| Health Care Service Corporation  Etc. (Average Information Technology (IT) Manager Salary, 2018) | Cyber Security Analyst | Cyber Security Analysts will analyze security system data, communicate security information and provide assistance to prevent malicious activity. | $50,961 - $117,574 |

Conclusion:

As shown above, even though the huge company with top talent and significant resources would love to be devoted to hire staff with highly command of Security and Certification. High salary is provided for the technique staffs. Although the need of Security and Certification staff is in need, it’s still hard to forecast with certainty the number of workers required or needed mic of security and certification knowledge skills. The security and certification workforce encompass a variety of contexts, roles, and occupations and is too broad and diverse to be treated as a single occupation or profession. Whether and how to professionalize will defer from role and context. Because security and certification is not solely a technical endeavor, a wide range of backgrounds and skills will be needed in an effective national cybersecurity workforce.

Reference:

(Payscale, 2018)<https://www.payscale.com/research/US/Job=Systems_Administrator/Salary>

(Payscale, 2018)<https://www.payscale.com/research/US/Job=Information_Security_Analyst/Salary>

(Average Information Technology (IT) Manager Salary, 2018)<https://www.payscale.com/research/US/Job=Information_Technology_Specialist/Salary>

[https://www.payscale.com/research/US/Job=Cyber (PayScale, 2018)\_Security\_Analyst/Salary](https://www.payscale.com/research/US/Job=Cyber_Security_Analyst/Salary)

Part 2 One-Time Pad (OTP) Research

Who was behind the initial idea

The well-known inventor of the OTP was Gilbert Vernam, who lent his name to the Vernam cipher. An IT engineer, he developed and patented a system for cryptography using punched tapes to store a randomized key. After though, the concept of the OTP had not been defined. The time when Vernam’s machine was found by Captain Joseph, Joseph set up lots of of the conditions necessary for an OTP nowadays, for example using a truly randomized key that would be destruct after one time usage. Although this type gained some usability from the commercial and the military sector, it also went hugly unnoticed.

When they were ﬁrst used

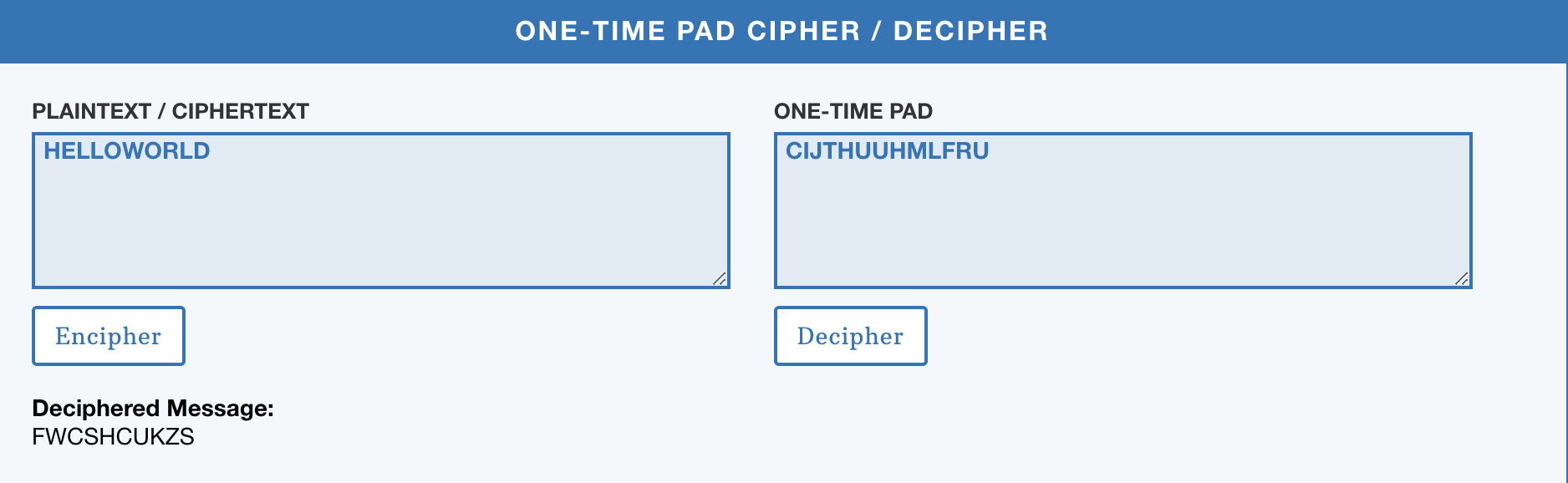
The first time that OTP was applied to the company usage was in the 1920s.They used the pen and paper system to make OTP. Pads of paper which would be ripped off and destroyed after use would print the random sequences of. Today, OTP format is most common in espionage operations, in which a small pad of paper can be separated into both parties. Then the second earliest usage of OTP is that the German government adopted the system in 1923

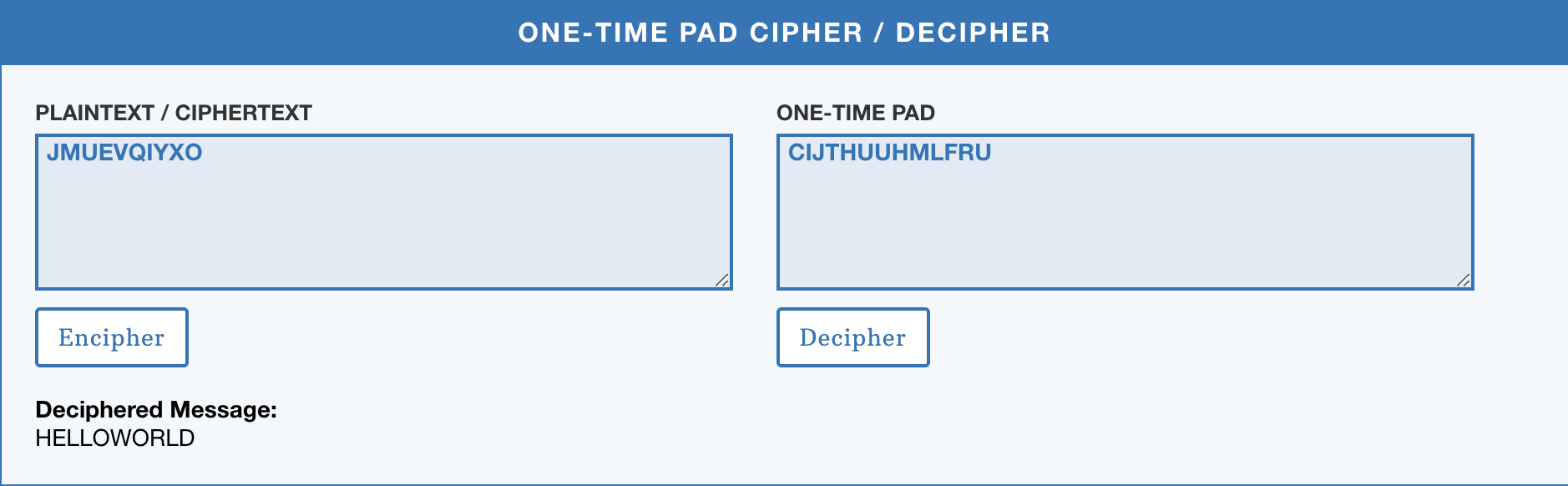
In what application they were found

Nowadays, OTP is largely used in bank field. When you go for any transaction involving mobile banking or Debit card payment, to authenticate the transaction, one system generated password. OTP will be sent to your mobile number registered with your Bank account. You are able to verify the transaction with this password or OTP.

How they are used today

The OTP is more a theoretical construction comparing to the construction of the real world. The OTP go through with 3steps: Key Generation, Key Distribution, Key Destruction. The first step is to generate a key. The hardware RNG doesn’t satisfy this in the practical. They almost always use the bits by using a hash function. What the expertise do is to design their own RNG to use only de-biasing techniques to maintain the security proof. Second step is to distribute key. However, it’s not easy to distribute only message information when you get a secure channel of transmitting the key. Thus the engineers create a pad which slightly overpowering/underpowering device to get duplicate photons, shinning a laser at the device to subtly break it or some other error inducing attack. Having received the key, the last steps for OTP is to destroy the key user received. At the time you have used a key, you should guarantee it’s properly destroyed in two both places. If it is not done correctly, users will lose the security to use the OTP. If the OTP number is not in deconstruction status after usage, it may be likely used twice or more. Then your information or property may be stolen by the hacker.





Would it be practical to use OTP

It’s practical to use OTP. (Thompson, 2016) OTP is used in many "quantum encryption schemes." Typically these schemes are actually standard one-time-pad encryption with the key being distributed using Quantum Key Distribution(QKD). They are impossible to be decrypted because there is no way to intercept the key due to quantum physics. Theoretically, this is useful for highly sensitive messages that need to remain secure for ever no matter what breaks in known cryptographic primitives happen or what advances in computational power (particularly quantum computing) occur. There are commercial QKD schemes, though I do not know how much they are actually used.

Part 3 Bring Your Own Device (BYOD) Policy

Introduction:

Having studied the BYOD and follow the two BYOD policy, a BYOD policy for JCU students and staffs are provided and listed below. The BYOD policy for JCU will assist teacher with improving education quality, release the pressure for JCU IT groups to maintain and manage the equipment in JCU and guarantee the safety of using device in campus.

BYOD policy for JCU: (Policy library, 2018)

1. Objectives - Policy statement

1.1

University, in consultation with their communities, is able to allow students to take their own personal electronic devices such as mobile pad to university for the aim of studying.

1.2

University -developed guidelines and deals for BYOD have to be connected to staff’s monitor, students, parents and caregivers.

1.3

The usage of private mobile or pad devices at university will help with studying, will be customized and student-centered, and will meet the requirement of teachers, students, parents and caregivers.

2. Audience and applicability

2.1

University professor, teacher, tutor, parents, caregivers and students.

3. Context

3.1

The increasing number of availabilities of private mobile equipment has boosted the need for new models of studying.

3.2

University has the right to harness students’ connection to their own personal mobile devices for the reason of developing nowadays learning skills and for fostering digital literacy and citizenship in a secure situation.

4. Responsibilities and delegations

4.1 The department

4.1.1

The department takes responsibility for the monitor and surveillance of its laptop systems to make sure the ongoing confidentiality, integrity and availability of university internet secure services.

4.2 The principal

4.2.1

The principal takes responsibility to develop g and to implement the university’s BYOD policy.

4.3 The student

4.3.1

The student is responsible for abiding by the school’s policy and the department’s Online Communication-Acceptable Usage for School Students.

5. Monitoring, evaluation and reporting requirements

5.1

The Information and Technology Directorate have the right and will keep maintenance and updating this policy when necessary.

What restrictions should be enforced (Berry, 2016)

1. Make Distinguish of Devices Whether Can Use or Not
2. Construct a Stringent Security Policy for all Devices Equipment.
3. Make a Service Policy for Devices and Equipment Under BYOD Standard.
4. Make It Purely Who Owns What Types Apps and Data (Thompson, 2016)
5. Make decision on What Apps Will Be Permitted or Banned.
6. Proofread Your BYOD Plan with Your Acceptable Use Policy.
7. Construct an Employee Exit Strategy.

What control should the organization have over the personal devices (Hassell, 2012)

Remote wipe and lock. The equipment should be kept safe. What if they are stolen and thief want to steal the important secret material inside the devices. The Remote wipe and lock will assist with solving the issues in this situation. Adding Remote wipe and lock function to the device will help you keep the data secure when the devices are out of your control.

Geo-location tracking. The Geo-location tracking will provide the information that the device route of being stolen. Geo-location tracking provides the possibility for you to seek the losing device. Once there is no back up for the data, Geo-location tracking will be the last hope for the device owner to track the device.

Network authentication, authorization, accounting will allow the computer user to use the device with the identification authorization. It will help the owner to decline the unauthorized user to steal data from the devices. It is of significance to have it on the computer especially for the public usage devices.

Secure remote support will assist user to solve the problem online instead of fixing it outside or calling from the other and. The service is convenient and improve the efficiency of problem finding and solving.

Acceptable use policy will enforce the user to read and accept the security policy before using the devices. Its purpose is to note the user what can be done and what is banned on using the devices. Having been educated and notified, users will take the knowledge of how to use and how to keep devices safety when using the public internet.

Part 4 Open Authentication (OAuth)

Introduction:

Recently OAuth is widely used in the real life’s app. For example, in new website’s registration, the website guide will lead you to login through Facebook or Gmail. In this section, author will guide you to take knowledge of what is the OAuth, the SWOT of OAuth, the comparison between OAuth and OpenID and OAuth usage in banking as well. (Grimes, 2017)

What is the technology behind it?

OAuth is using an open-standard authorization protocol or as the framework that allow the servers and services to connect with certain authorization without actually sharing the personal information and credential. The term will be described as secure, third-party, user-agent, delegated authorization in the authentication parlance.

What are its strength? (Fronczak, 2011)

There are lots of merits for OAuth. Its convenience improves the efficiency for the user when use the application during log in time. For example. If you received a video or the picture that you want make a comment on from your friends. What make you in dilemma is that you have never been to the website and don’t have the account as well. The time when you consider whether it’s worth for you to take time to do the registration for the website, you find a button log in with google or Facebook account. Then you can easily access to the account without do registration again. Numbers of Facebook, Google, Twitter users in the world, they you the same convenient way to log in and finish registration from unknown website. Form this perspective OAuth saves time for users. Secondly, OAuth allows you to use one account to comment on several different sites, letting friends and readers from all sites trace you back to your preferred profile page. That makes it easier for people to do social networking on the internet. The OAuth solves problem of personal privacy as well. OAuth allows you to login to site A to leave a comment on site B, the same is true for hiding your banking information from those you do business with online. When making a payment all you need to do is use OAuth to login to your online bank account and have the transaction occur without the clothing site ever knowing your credentials information, which means although user log in to the website every time, however the website holder is not access to your personal information. Recently, the latest version of OAuth released – OAuth 2.0. All OAuth data transfers must take place on SSL (Secure Sockets Layer) to ensure the most trusted cryptography industry protocols are being used to keep data as safe as possible. It’s easier and better to take measures to protect secure for users. Nowadays, OAuth is widely used. Large Tech company like Google, Facebook, Twitter, and Yahoo used OAuth to give availability permission to the website. It’s popularity makes user’s preference to use it as well.

What are its weaknesses? (Fronczak, 2011)

Although OAuth brings lots of benefits for the user, there are lots of cons for using OAuth as well. The most severe one is lack of anonymity. If you use Facebook to comment on a different site, they can not only see your Twitter avatar icon, but also click on you to see who your online friends are. It’s a choice the user has to be comfortable making, and with most Internet users still preferring to make comments anonymously on the Web, it’s a choice many still aren’t prepared to make yet. Needing to make anonymous alternate accounts can be just as annoying as having to toggle dozens of site privacy settings each month. And the other problem could be that OAuth is easy to use as phishing. Many unfortunate users will inevitably fall victim to a convincing looking popup ad and have their data phished when using OAuth. It’s need to be education that how to use OAuth correctly.

Will it replace OpenID?

OpenID Connect provides a way for the application to retrieve information about the authenticated user. Most importantly it provides a level of assurance that the information is valid (as far as the authorization server is concerned anyway). This can then be used to facilitate identity federation. While OAuth is an authorization protocol, providing a way to give authorization to access a protected resource. A by-product of the authorization process is that the user is authenticated.

Technically, OAuth does not have to give you any information about the user. What it provides is a validation that the user has given authority to the application to access some data. This is governed by the scope of the authorization grant. People can be achieved with OAuth by granting a scope that allowed access to the user's identity information. OpenID Connect standardizes that scope.

Would you recommend it for secure applications like online banking?

Although OAuth has lots of merit, it’s not recommended to use as banking service. Attacks such as Man-in-the-middle will break the system security and destroy the balance between users and bank authorizations. One of the biggest issues in OAuth 2.0 is that OAuth 2.0 heritage all security problems of SSL. The pain point is that only the user authenticates the server, the server doesn't authenticate the client. The user does this by providing SSL certificate. This means the server will never take the knowledge of who is sending the request at the moment. The most realistic potential problem is the user developer not properly identifying the server authentication.

Part 5 Cryptanalysis of Substitution Ciphers:

Introduction:

In this section, author will using keyword frequency comparison to decrypt monoalphabetic (substitution) cryptographic system. The explanation will be stated in the following steps.

Cipher Text

Cryptogram for whom their Student-ID is XXXXXXX8

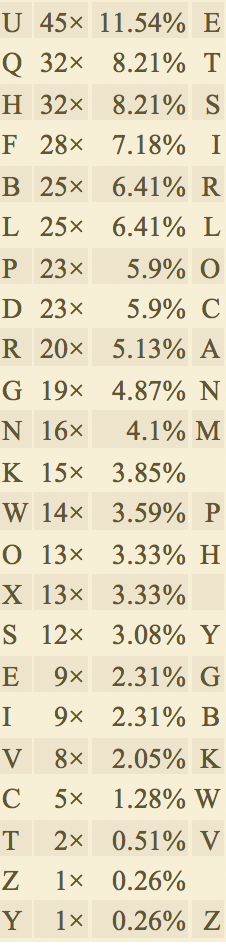
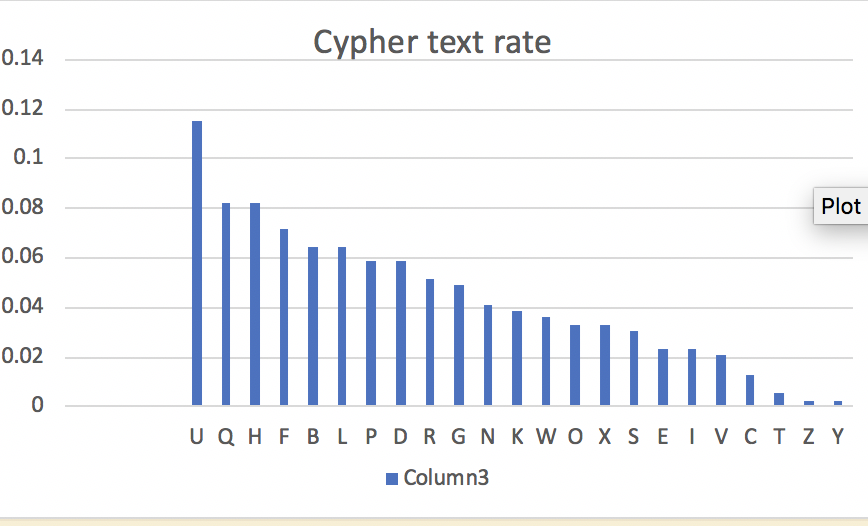
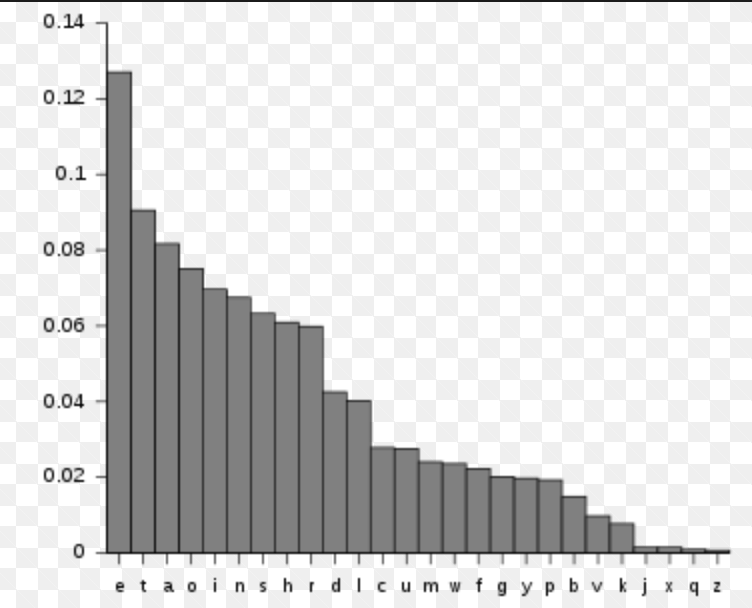
bftuhq, hornfb rgk rklunrg hopcuk opc qou zrdqpbfhrqfpg wbpilun dpxlk iu xhuk qp dpghqbxdq r wxilfd-vus dbswqphshqun (qofh fh qou cull-vgpcg bhr dbswqphshqun). nubvlu rgk oullnrg xhuk qou vgrwhrdv wbpilun fg qoufb dpghqbxdqfpg. ndulfudu ixflq r hshqun cofdo rwwlfuk ubbpb dpbbudqfge dpkuh. lrqub fg 1985, ulernrl kuhfeguk r wxilfd-vus dbswqphshqun xhfge qou kfhdbuqu lperbfqon wbpilun. nfllub rgk vpilfqy hxeeuhquk xhfge ullfwqfd dxbtuh qp kuhfeg wxilfd-vus dbswqphshqunh.

Methods:

According to statistics, there are totally 23 letters in use. And letter X, Q, Z, J are not in the cipher text. Illustrate 5.2 is the frequency of English letter in English text. Illustrate 5.3 is the letter frequency in the cipher text. We can decrypt the cipher text by using the frequency comparison between two illustrates. For example, the highest frequency letter in English text is E while the highest frequency in cypher text is U, both of which has the frequency reach to 12%. Consequently, we have high confidence that the letter U in the cipher text should be the letter E in the plain text.

Keyword table:

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

* 1. 5.2 5.3

Decrypted Plaintext for the cipher text:

Rivets Shamir and Adelman showed how the factorization problem could be used to construct a public-key cryptosystem (this is the well-known RSA cryptosystem). Merkle and Hellman used the knapsack problem in their construction. McElwee built a system which applied error correcting codes. Later in 1985, Ellamae designed a public-key cryptosystem using the discrete logarithm problem. Miller and Knoblets suggested using elliptic curves to design public-key cryptosystems.

Reference:

PayScale E Salary for Certification: CompTIA Security+(2018)

<https://www.payscale.com/research/US/Certification=CompTIA_Security%2B/Salary>

PayScale E Average Systems Administrator Salary: CompTIA Security+(2018)

<https://www.payscale.com/research/US/Job=Systems_Administrator/Salary>

PayScale E Average Network Engineer Salary(2018)

<https://www.payscale.com/research/US/Job=Network_Engineer/Salary>

PayScale E Salary for Certification: CompTIA Security+(2018)

<https://www.payscale.com/research/US/Job=Information_Security_Analyst/Salary>

PayScale E Average Information Security Analyst Salary(2018)

<https://www.payscale.com/research/US/Job=Information_Technology_(IT)_Manager/Salary>

PayScale E Average Information Technology Specialist Salary(2018)

<https://www.payscale.com/research/US/Job=Information_Technology_Specialist/Salary>

PayScale E Average Information Technology Specialist Salary(2018)

<https://www.payscale.com/research/US/Job=Cyber_Security_Analyst/Salary>

Tom P. Is OTP useful in modern electronic communication?(2013)

<https://crypto.stackexchange.com/questions/11009/is-otp-useful-in-modern-electronic-communication>

Jane S. History of the One Time Pad(2010)

<http://introspectivenetworks.com/history-of-the-one-time-pad/>

Megan Berry BYOD Policy (2018)

<http://www.itmanagerdaily.com/byod-policy-template/>

Joel Snyder 5 Elements That Should Be in Every Organization’s BYOD Policy(2018)

<https://insights.samsung.com/2018/07/13/5-elements-that-should-be-in-every-organizations-byod-policy/>

NSW Education Student Bring Your Own Device Policy (BYOD)(2013) <https://education.nsw.gov.au/policy-library/policies/student-bring-your-own-device-policy-byod>

Keith W. Miller ; Jeffrey Voas ; George F. Hurlburt BYOD: Security and Privacy Considerations(2012)

<https://ieeexplore.ieee.org/abstract/document/6320585>

Rafael Ballagas1 , Michael Rohs2 , Jennifer G. Sheridan3 , and Jan Borchers1BYOD: Bring Your Own Device(2004)

<http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf>

Jonathan Hassell Establishing a Successful BYOD Policy(2012) <https://www.cio.com/article/2395944/consumer-technology/7-tips-for-establishing-a-successful-byod-policy.html>

D. Hardt, Ed.The OAuth 2.0 Authorization Framework（2012）

https://www.rfc-editor.org/rfc/rfc6749.txt

M. Jones The OAuth 2.0 Authorization Framework: Bearer Token Usage(2012)

<https://www.rfc-editor.org/rfc/rfc6750.txt>

Cynthia Bunting Protect Your Company From Employee Devices(2015)

<https://www.businessnewsdaily.com/1566-employee-device-security.html>

Roger A. Grimes What is OAuth? How the open authorization framework works(2017)

<https://www.csoonline.com/article/3216404/authentication/what-is-oauth-how-the-open-authorization-framework-works.html>

Tom Fronczak OAuth: Pros and Cons of OAuth(2011)

<http://www.socialtechnologyreview.com/articles/oauth-pros-and-cons-oauth>

Josh Mandel Introducing TAuth: Why OAuth 2.0 is bad for banking APIs and how we're fixing it (2016)

<https://news.ycombinator.com/item?id=11636847>