

|  |
| --- |
| JCU |
| CP3404 Assessment |
| Cairns Cheng Peng |

|  |
| --- |
| 11-1-2019 |

Table of Contents

[Introduction 4](#_Toc23712659)

[Security+ Certification Jobs That Make You a Millionaire 4](#_Toc23712660)

[Abstract 4](#_Toc23712661)

[Keywords 4](#_Toc23712662)

[Introduction 4](#_Toc23712663)

[Solution 4](#_Toc23712664)

[Summary 6](#_Toc23712665)

[Use One-Time Pad (OTP) to Make Your Life Easier 6](#_Toc23712666)

[Abstract 6](#_Toc23712667)

[Keywords 6](#_Toc23712668)

[Introduction 6](#_Toc23712669)

[The Man Behind the Initial Idea 6](#_Toc23712670)

[The Time OTP First Used 7](#_Toc23712671)

[Application OTP Found 7](#_Toc23712672)

[OTP Today Usage 7](#_Toc23712673)

[OTP Practice 8](#_Toc23712674)

[Practical OTP Usage 8](#_Toc23712675)

[Summary 9](#_Toc23712676)

[Bring Your Own Device (BYOD) Policy 9](#_Toc23712677)

[Abstract 9](#_Toc23712678)

[Keywords 9](#_Toc23712679)

[Introduction 9](#_Toc23712680)

[BYOD Policy Designed for JCU 9](#_Toc23712681)

[Restriction Should be Enforced 10](#_Toc23712682)

[Control that Organization Have Over the Personal Devices 10](#_Toc23712683)

[Summary 11](#_Toc23712684)

[Open Authentication (OAuth) is Around your Life 11](#_Toc23712685)

[Abstract 11](#_Toc23712686)

[Keywords 11](#_Toc23712687)

[Introduction 11](#_Toc23712688)

[The Technology Behind OAuth 11](#_Toc23712689)

[OAuth Strength 12](#_Toc23712690)

[OAuth Weakness 12](#_Toc23712691)

[OAuth 1.0 12](#_Toc23712692)

[OAuth 2.0 12](#_Toc23712693)

[The Possibility of Replacing OpenID 13](#_Toc23712694)

[Recommendation For secure application like Online Banking 13](#_Toc23712695)

[Summary 13](#_Toc23712696)

[Ancient Cryptanalysis of Substitution Ciphers Open Your Mind 14](#_Toc23712697)

[Abstract 14](#_Toc23712698)

[Keywords 14](#_Toc23712699)

[Introduction 14](#_Toc23712700)

[Cipher Text 14](#_Toc23712701)

[Decrypt Cipher Text Solution 14](#_Toc23712702)

[Methodology Applied 14](#_Toc23712703)

[Letter Frequency Analysis and Comparation 14](#_Toc23712704)

[Statistic of Letter Frequency in Normal Text (Appendix Page) 15](#_Toc23712705)

[Statistic for Cipher Letter of Text (Appendix Page) 15](#_Toc23712706)

[Graphic for Cipher Letters and Normal Letters (Appendix Page) 15](#_Toc23712707)

[Comparation and Solution 15](#_Toc23712708)

[Summary 15](#_Toc23712709)

[Appendix 15](#_Toc23712710)

[Keyword Table Blank 15](#_Toc23712711)

[Keyword Table Finished 15](#_Toc23712712)

[Statistic of Letter Frequency in Normal Text 16](#_Toc23712713)

[Statistic for Cipher Letter of Text 17](#_Toc23712714)

[Graphic for Cipher Letters and Normal Letters (Appendix Page) 18](#_Toc23712715)

[Reference 19](#_Toc23712716)

# Introduction

Information Security problems these days became a necessary and pressing drawback to be solved throughout the data revolution era. Consequently, to command the mandatory talent and data security-related ideas is of quite significance. The report is aimed to assist with raising the notice of data security in real utility, problem-solving, and important thinking improvement. The Google search engine is used to search out the best-matched answer on the Google Scholar or connected Scientific web site to unravel Job handiness, Security Policy, Authentication, cryptography and decoding issues. The paper is going to be directed into five sections. within the initial section, accessible job positions that need security and certification likewise as their connected introductions will be listed to assist job finders to acquire available job offered on the market. Within the second section, the author can tell you what's One Time Pad (OTP) and its application these days. An endeavor on exploitation OTP will be conducted as well. Then within the third topic, a BYOD policy for JCU will be drafted for security. Forth part follows with an associate introduction to Open Authentication (OAuth) as well the process of cooperation with partner to decode. Finally, the last part deciphers methodology of code that encrypted with substitution cipher mistreatment English letter Frequency Comparison methodology will be applied.

# Security+ Certification Jobs That Make You a Millionaire

## Abstract

This section attaches significance on providing suitable and reliable Security+ Certification Jobs for employers who want to devoted themselves to information security field as their career.

## Keywords

Security Jobs, Certification Jobs, Employer, Millionaire, Salary, Information Security.

## Introduction

The necessity for certifications has become a truth of life for data Technology (IT) professionals. Nearly any position posting encountered can list some certification requested or needed. However, the extent and nature of certification valuation by employers remains unclear. Past analysis is proscribed and has examined the relationships between certifications and job skills and education. whereas necessary, the present analysis provides largely anecdotal support for the worth of and acquisition of certifications. The analysis focus of this text is to provide several Jobs available for Security and Certification Jobs with its description and salary. As well. It is of significance for IT guys to search out a correct job associated with certification and security. The table below is able to provide the foremost well-liked jobs associated with security and certification. Additional information like associate degree leader, job title, description of the task and remuneration vary are offered as a respect to assist you to reach an honest job associated with Security and Certification. security.

## Solution

|  |  |  |
| --- | --- | --- |
| job title | description of the job | Salary range |
| Security Consultants Relations Manager [1] | The construction industry is changing, cybersecurity has become a key consideration when securing access points in buildings often designed in BIM that have more and more compliance requirements. To accompany this, change this position requires a knowledgeable and experienced business professional to increase HID Global’s specification sales opportunities and image within the consultants/engineers/specifier’s community. The actions of this position will result in HID Global being the “Trusted Advisor” to specifiers and creating pull-through sales of HID Global’s hardware and cloud solutions. The professional shall feel comfortable being the “voice of HID” in front of senior managers, decision makers and convey HID’s corporate vision and strategy. | AU$88k - AU$159k |
| Certified Ethical Hacker (CEH) [2] | Also known as Certified Network Defense Architect (CNDA) for government employees, this is obtained through the EC-Council and requires participants to have two years of experience in the information technology industry before taking the exam. Having your Security+ is a huge plus here as the goal of this certificate is to get you thinking like a hacker so you can thwart attacks against your employer. | $46,849 - $102,602 |
| Security Manager [3] | Security managers are employed in a range of industries, from retail to computer technology. Because the work can vary greatly, some employers require that applicants have a bachelor's degree in management, while others prefer work experience over education; this is a managerial position, so most employers require anywhere between three and ten years of experience. [4] | AU$56k - AU$143k [3] |
| Certified Information Systems Security Professional (CISSP) [5] | CISSP is an advanced-level cybersecurity certification put out by (ISC)2. It focuses on cybersecurity management skills. | $110,142 - $119840  [6] |
| Information Technology Specialist | Information technology specialists work closely with a range of technology product, from their style to regular repair and maintenance. | $35,515 - $95,571 |
| Cyber Security Analyst | A cybersecurity analyst either works directly for an organization as a staff member or as a consultant, possibly working for several companies at any given time. The title cybersecurity analyst is just one variant. Similar roles and titles include information security analyst, security operations centre (SOC) analyst and security analyst. They all basically have the same job description and carry out the same tasks. As a security analyst, your overriding duty is to implement systems that protect your organization from the spectre of cyberthreats. What this means, in reality, is a list of tasks that come together to perform that duty. [7] | $50,961 - $117,574 |

## Summary

In the cyber realm, security+ certification employers are the go-to professionals for alert triage and event analysis. So, what it takes to get security+ certification jobs are to have formal education in IT, computer science, or cybersecurity; he or she will also have on-the-job experience and, preferably, professional certifications. [8]

With the growing need for intrusion prevention and data collection for intelligence, many of the new professionals formed for the new IT era are bound to be security+ certification. Protecting the integrity of data and the security of the systems are a vital necessity for any organization, and that is why the need for cybersecurity analysts will surge in the next few years.

# Use One-Time Pad (OTP) to Make Your Life Easier

## Abstract

The one-time pad, the mother of all encoding schemes, is accepted to be information-theoretically secure, in distinction to most encoding schemes employed in follow, that area unit at the most computationally secure. In this section, the background story of How OTP was invented, OTP’s usage as well as its Application is going to be demonstrated.

## Keywords

OTP, Gilbert Vernam, First time, Background story, OTP Usage.

## Introduction

One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. It is the only existing mathematically unbreakable encryption. The following paragraphs is going to date back to the time that how OTP was invented as well as its inventor’s story. OTP’s first usage and nowadays OTP applications.

## The Man Behind the Initial Idea

The story of one-time pad began in 1882, when the Frank Miller, the Californian banker, assembled his "Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams". This codebook was widely used, for reducing telegraph costs by putting words and phrases into short letter-codes or number-codes. These codebooks didn’t provide enough security for the information. But Miller's codebook provided instructions for a super encipherment (a second encipherment layer over the code) by an unique method: he added some shift-numbers which is called key nowadays to the plain code (words, converted into a number) and defined the shift-numbers as a list of irregular numbers that should be erased after use and never be used again.

Time fly’s to Vernam’s era. In 1917. AT&T research engineer Gilbert Vernam developed a system to encrypt teletype TTY communications. Vernam reckoned that encryption with short key tapes (basically a poly-alphabetic cipher) would not provide security enough. At the begining, Vernam used a combination of two key tape loops, with same length, creating one long enough random key. Captain Joseph Mauborgne said that even the double key tape system was not able to resist cryptanalysis if large amount of message traffic were encrypted. Mauborgne drew conclusion that only if the key tape was unpredictable, the message will be used only once, the message would be secure. Moreover, the encryption gave conclusion that it was unbreakable. One-time encryption was created.

. The production, distribution and consumption of enormous quantities of one-time tapes limited its use to fixed stations (headquarters or communications centres). It was not until the Second World War that the US Signal Corps widely used the OTT system for its high level teleprinter communications. However, three German cryptologists did immediately recognize the advantages of one-time encryption.

## The Time OTP First Used

The first time that OTP was applied to the corporate usage was within the 1920s. NSA called Vernam's 1919 one-time tape (OTT) patent "perhaps one of the most important in the history of cryptography" (Melvin Klein, NSA). AT&T marketed the Vernam system in the 1920s for commercial secure communications, albeit with little success. At that time, the German cryptologists Werner Kunze, Rudolf Schauffler and Erich Langlotz cryptanalyzed French diplomatic traffic. These pencil-and-paper numerical codes used code books to transfer words and phrases. Short repetitive numerical key (by modulo 10) to encrypt the code book values by Freches. The German cryptologists had no problem in breaking these short keys but thought that adding a unique random key digit to each individual code group digit would leave the message unbreakable. They changed a system with paper sheets containing random numbers. Each number was in use once only. And the sheets, of which there were only two copies (one for sender and one for receiver), should be destroyed after use. In fact, they re-invented Frank Miller's 1882 system. [9]

## Application OTP Found

Recently, OTP is widely used in technology and life we are experiencing. There are several general applications that can be found using frequently these years, including, financial, political, educational, medical as well as information security field.

1. Banks and Finance companies are in need for sending OTP to their customer. (Ex: AXIS OTP)
2. Government agencies to verify the citizen directory.
3. Travel and Tourism companies to check the right customers.
4. Online home delivery of any product to confirm about right customer.
5. To verify mobile number an OTP is sent to registered mobile users while downloading an app
6. Useful for Ecommerce online portals for user verification at the time of payment.
7. IT company, Finance Company, Healthcare industry and Training Centres.
8. Schools, Collages and Hospitality. [10]

## OTP Today Usage

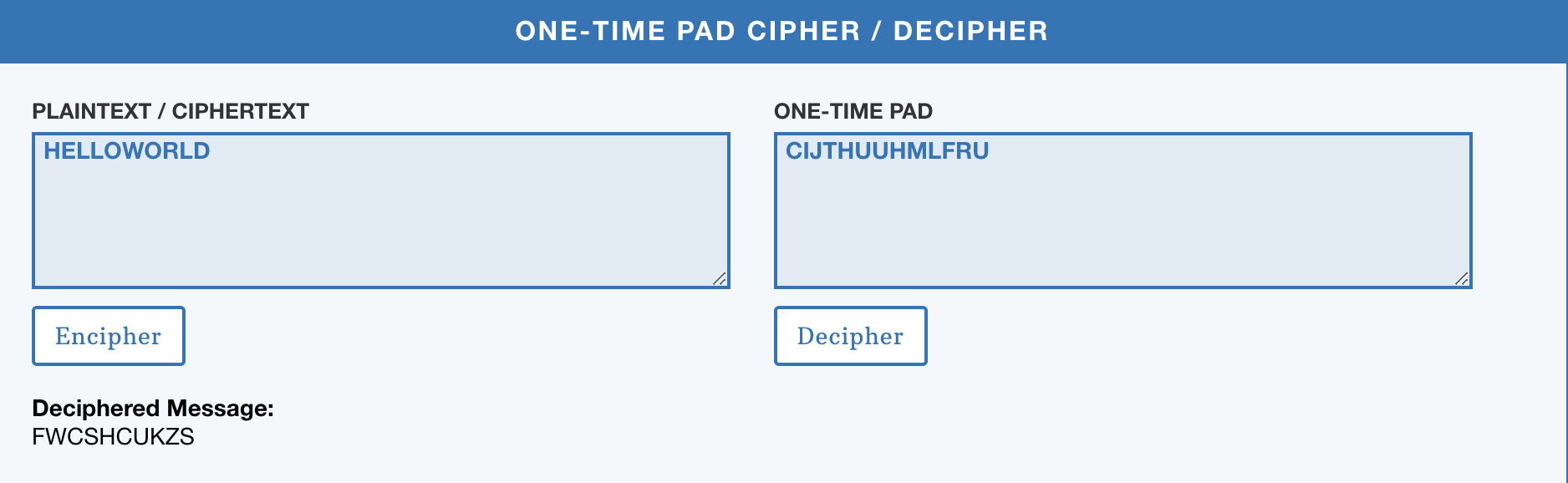
The OTP is widely used in today’s life. OTP has penetrated into financial, education, communication fields already. The OTP go through with 3steps: Key Generation, Key Distribution, Key Destruction. The first step is to generate a key. The hardware RNG doesn’t satisfy this in the practical. They almost 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.

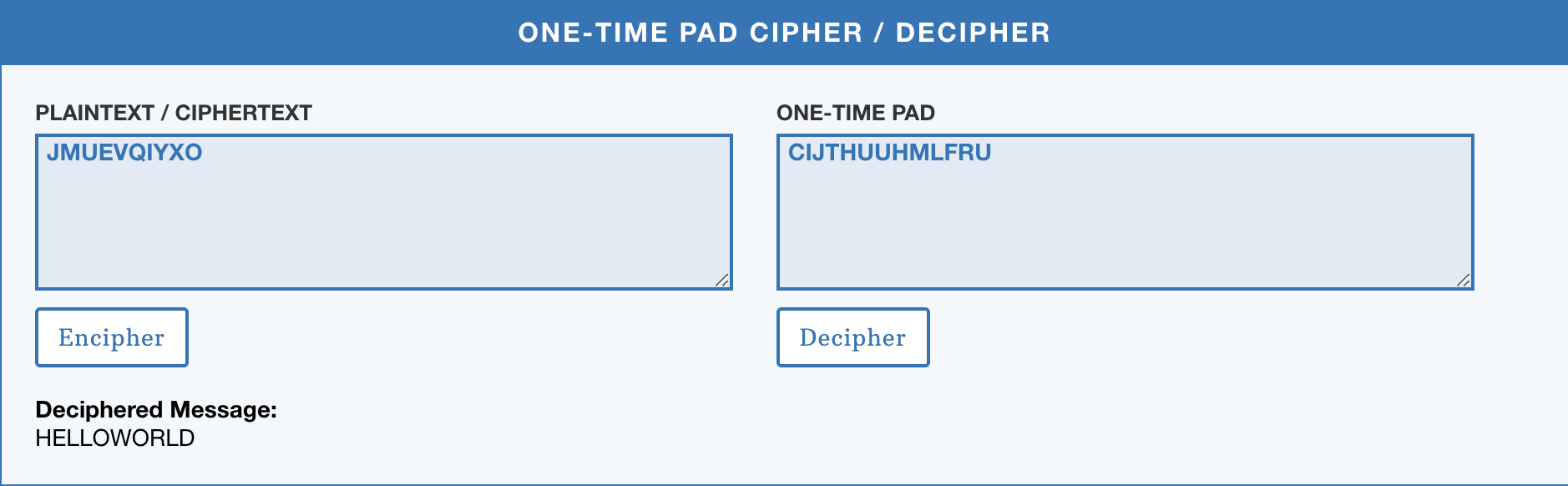
## OTP Practice

Below is the practice history with partner.

We pass the One -Time Pad to each other and use OTP to decipher the cipher text. There are three steps for OTP usage. We generate the OTP key first. Having generating the key, we send the key to each other, which is so-called key distribution. Having got the key he sends to me, I used key to decipher the text. After deciphering the text, the key was destroyed by refreshing the page.

Finally, “Hello World” was the message that he wants to send to me.





## Practical OTP Usage

OTP is practical to use during these days and it’s even widely 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, theoretically unbreakable since there is no way to intercept the key thanks to quantum physics (in practice, there are some problems). In theory, this is useful for highly sensitive messages that need to remain secure forever no matter what breaks in known cryptographic primitives happen or what advances in computational power (particularly quantum computing) occur.

## Summary

From the perspective list above. Not only the invention history story is interesting, but also the OTP utility fill our life with colorful and convenient world. An OTP is more secure than a static password, especially a user-created password, which can be weak and reused across multiple accounts. OTPs may replace authentication login information or may be used in addition to it in order to add another layer of security.

# Bring Your Own Device (BYOD) Policy Make Study Live Easier

## Abstract

Bring your own devices (BYOD) refer to the practice where users using their own devices or personal gadget in the organization or institution to complete their task. Nowadays, users bring different types of internet-ready device; not limited to the end-user devices like a laptop, tablet, smartphone, smartwatch and other wearable devices. Some of them also come with network-level devices such as personal or small office home office wireless router and other Bluetooth enabled devices. In the university campus environment, BYOD practice provides significant advantages for both users and university. Students may have unlimited access to internet resources for their needs includes the education and social benefits whereas for the university, BYOD implementation can help to reduce the cost of devices’ maintenance.

## Keywords

BYOD, Security, Policy, User’s Awareness.

## Introduction

BYOD (Bring Your Own Device) emerged some years ago as a change in the way organizations provided access to their computer networks. [11] Traditionally the Information Technology (IT) department of a business or school would build closed networks that only the computers they owned could access. BYOD allows employees and students to also join their own computers, smartphones, and tablets to these more open networks. In this section, BYOD policy for JCU will be created by referencing two different organization’s BYOD policy. That the restriction that the company should put in force on the device that taken and the control the company should have on the device that taken will be discussed on the following topic as well.

## BYOD Policy Designed for JCU

* Objectives - Policy statement
  + Students are allowed to bring their own personal electronic devices like pad, mobile, laptop to the university for the aim of usage of learning or other related way to assist studying.
  + Staff’s monitor, parents and caregivers as well as student’s device should connect to university – developed user guidelines and deal for BYOD.
  + The utility of private laptop, pad and cell phone devices at university will assist with learning, will be students centred and customized, and will meet the need of teachers, students, parents and caregivers.
* Audience and applicability
  + University professor, students, parents, caregiver’s teacher, tutor and visitors.
  + All the proper user should come from the list above. Dangerous users should be blocked.
* Context
  + Large amount of availabilities of private mobile devices have been improved the requirement for new models of leaning.
  + University has the right to stop students’ connection to their own personal electronical devices for the reason of developing nowadays practicing skills and for fostering digital literacy and citizenship in a required situation.
* Responsibilities and delegations [12]
  + The department
    - 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.
  + The rules
    - The principal takes responsibility to develop g and to implement the university’s BYOD policy.
  + The users
    - The user is responsible for abiding by the school’s policy and the department’s Online Communication-Acceptable Usage for School Students.
  + Monitoring, evaluation and reporting requirements
* The IT Directorate have the ability and is going to keep maintenance and refreshing this policy when need.
  + The IT Directorate have the right and will keep maintenance and updating this policy when need
  + University need to inform user in advance when there is updating issue for the pausing of usage of internet connection.

## Restriction Should be Enforced

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
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.

## Control that Organization Have Over the Personal Devices

With 73% of internet consumption in 2018 coming from mobile devices, security surrounding their business usage is more crucial than ever. Some things to consider are:

1. Setting up a virtual desktop infrastructure (VDI) [13] or mobile device management protocol to ringfence the company data from personal data. Private cloud storage is also a viable option. This ensures not only is the company-owned information protected from outside access, it keeps the employee's personal data private.
2. Requiring strong passwords, time-out locking, certain company-provided anti-virus and [14]protective software, and setting up protocols for reporting a lost or stolen device right away. Encouraging regular backups can also help.
3. Transparency about company access and monitoring of employee devices. When an employee leaves the company or transfers to a department where their permissions change, there will be no surprises about what does and doesn't get wiped from the employee's device. Before allowing access to the company data, be sure all parties, including management and IT, are explicitly clear on the policy rules. If there's crossover between company access into personal data, state how the company will protect that personal information, and within what limits that protection is expressly stated.
4. Considering cyber liability insurance. Sometimes, no matter how secure a device or network is, hackers can get through. Knowing your legal rights and responsibilities, as well as ensuring any breaches can be handled within state and industry regulations, you can be assured you and your employees are covered in the event of a threat.

## Summary

BYOD, then, is of course a model that can be operated with several moderate tweaks to a university or school. The main problem is planning, particularly for infrastructure part and support. [15] However, once this has been applied, students not only get the freedom to bring their own device, but are affordable to the space for a flexible and enthusiastic approach to their studying. This is absolutely much more valuable cargo than books and pencils.

# Open Authentication (OAuth) is Around your Life

## Abstract

OAuth is an open-standard authorization protocol or framework that describes how unrelated servers and services can safely allow authenticated access to their assets without actually sharing the initial, related, single logon credential. In authentication parlance, this is known as secure, third-party, user-agent, delegated authorization. Company like Twitter and Google [16] even Facebook, use OAuth to grant user to use their account to login to third party website without registration. OAuth definitely bring lots of convenience to our life.

## Keywords

OAuth, Open Authentication, Story, Pros, Cons

## 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. This section will explain the technique used in OAuth, OAuth’s pros and cons along with recommendation for secure application like Online Banking.

## The Technology Behind OAuth

OAuth protocol is an outsourced authentication protocol, masterminded by the authenticating server. It is different from OpenID or other federated identity protocols in that OAuth accepts only a single set of credentials whereas OpenID accepts multiple sets of credentials (Yahoo id, Google id, etc.). OAuth allows the task of authentication to be performed by the one component that can authenticate the user and is in fact, in charge of it - the authentication server - even though 3rd party components (called clients) request for the authentication. [17]

Once a service becomes a platform, 3rd parties create applications that operate on the platform. These applications need access to protected resources on the platform, which has a set of credentials to authenticate a user. However, creating application-specific credentials to authenticate the user is not optimal - e.g. for each application on the Twitter platform, it is impractical to ask a twitter user to enter application-specific username and password. Alternatively, giving platform credentials to the 3rd party application is not secure either. OAuth addresses this problem by authenticating the user with the platform and allowing the 3rd party application to access the protected resources on behalf of the user.

There are 3 distinct parties involved in the OAuth interaction.

1. resource owner - e.g. the end user with credentials on the platform (aka "the server").
2. client - e.g. the 3rd party application, which is acting on behalf of the resource owner to access protected resources on the platform ("the server")
3. server - protected resource resides here. Additionally, the server can authenticate the resource owner.

## OAuth Strength

Going by the adoption rate, OAuth 2.0 is definitely an improvement over its arcane predecessor. Instances of developer community faltering while implementing the signatures of 1.0 are not unknown. OAuth 2.0 also provides several new grant types, which can be used to support many use-cases like native applications, but the USP of this spec is its simplicity over the previous version. [18]

## OAuth Weakness

### OAuth 1.0

1. Signing Every Request: Having the client generate signatures on every API request and validating them on the server every time a request is received, proved to be major setback for developers, as they had to parse, encode and sort the parameters before making a request. OAuth 2.0 removed this complexity by simply sending the tokens over SSL, solving the same problem at network level. No signatures are required with OAuth 2.0.
2. Addressing Native Applications: With the evolution of native applications for mobile devices, the web-based flow of OAuth 1.0 seemed inefficient, mandating the use of user-agents like a Web Browser. OAuth 2.0 have accommodated more flows specifically suitable for native applications.
3. Clear Separation of Roles: OAuth 2.0 provides the much-needed separation of roles for the authorization server authenticating and authorizing the client, and that of the resource server handling API calls to access restricted resources.

### OAuth 2.0

1. Interoperability: Adding too many extension points in the spec resulted in implementations that are not compatible with each other, what that means is that you cannot hope to write a generic piece of code which uses Endpoint Discovery to know about the endpoints provided by the different implementations and interact with them, rather you would have to write separate pieces of code for Facebook, Google, Salesforce and so on. Even the spec admits this failure as a disclaimer. [19]
2. Short Lived Tokens: The spec does not mandate the lifetime and scope of the issued tokens. The implementation is free to have a token live forever. Although most of the implementations provide us with short-lived access tokens and a refresh token, which can be used to get a fresh access token.
3. Security: The spec just "recommends" the use of SSL/TLS while sending the tokens in plaintext over the wire. Although, every major implementation has made it a requirement to have secure authorization endpoints as well require that the client must have a secure redirection URL, otherwise it will be way too easy for an attacker to eavesdrop on the communication and decipher the tokens.

## The Possibility of Replacing 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.

## Recommendation For secure application like Online Banking

Although OAuth has lots of merits, 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.

## Summary

OAuth is actually a good way to be applied in account authorization filed. And as you can see, it’s widely used in various of filed today. However, for some area, such as Online Backing service, it’s not recommended to use OAuth due to its shortcoming of easily being attacked. But each method has its own set of benefits and shortcomings. Theoretically, there is no right or wrong choice here – it doesn’t really matter what option decision maker makes an end up choosing, what matters is whether or not the method decision maker chooses matches client requirement. Consequently, it’s of significance to choose an approach that matches requirement.

# Ancient Cryptanalysis of Substitution Ciphers Open Your Mind

## Abstract

The MonoAlphabetic Substitution Cipher is a cipher that has been in use for many hundreds of years. It basically consists of substituting every plaintext character for a different ciphertext character. It differs from the Caesar cipher in that the cipher alphabet is not simply the alphabet shifted, it is completely jumbled. The simple substitution cipher offers very little communication security, and it will be shown that it can be easily broken even by hand, especially as the messages become longer (more than several hundred ciphertext characters).

## Keywords

MonoAlphabetic Substitution Cipher, Keyword table, Keyword, Frequency, Cipher

## Introduction

In this section, keyword frequency comparison is used to decrypt monoalphabetic (substitution) cryptographic system. The keyword table will support to find out the corresponding plain text and cipher text. A MonoAlphabetic Substitution Cipher maps individual plaintext letters to individual ciphertext letters, on a 1-to-1 unique basis. That is, every instance of a given letter always maps to the same ciphertext letter. The oldest such cipher known is the Caesar cipher, where the mapping involved a simple shift within the alphabet. The explanation will be stated in the following steps.

## Cipher Text

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.

## Decrypt Cipher Text Solution

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.

## Methodology Applied

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.

## Letter Frequency Analysis and Comparation

The statistic of frequency of the letter and the comparison between cipher text and plain text are listed in below tables:

### [Statistic of Letter Frequency in Normal Text (Appendix Page)](#_Keyword_Reference_Table)

### [Statistic for Cipher Letter of Text (Appendix Page)](#_Statistic_for_Cipher_1)

### [Graphic for Cipher Letters and Normal Letters (Appendix Page)](#_Graphic_for_Cipher)

## Comparation and Solution

Having calculated all frequency rate and compared cipher text and plain text, we can easily access the [Keyword Table](#_Keyword_Table) Blank. Keyword can finally be generated, which is “RELATION” for this part of cipher text [Keyword Table Finished](#_Keyword_Table_Finished). Then what is next to do is to write down all the letter except keyword in alphabet order across the table.

## Summary

MonoAlphabetic Cryptography is a powerful tool to protect information, especially when this is exposed to insecure environments such as the Internet. Historically, it mainly aimed at providing confidentiality. Intuitively, cryptography amounts to transforming a plaintext into a ciphertext so that unauthorized users cannot easily reconstruct the plaintext.

# Appendix

### Keyword Table Blank

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

[Return Back](#_Methodology)

### Keyword Table Finished

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R= A | E = G | L = L | A = Q | T = V |
| I = B | O = H | N = M | B = R | C = 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 |  |  |  |  |

[Return Back](#_Methodology)

### Statistic of Letter Frequency in Normal Text

|  |  |
| --- | --- |
| Letter | Frequency |
| E | 12.70% |
| T | 9.06% |
| A | 8.17% |
| O | 7.51% |
| I | 6.97% |
| N | 6.75% |
| S | 6.33% |
| H | 6.09% |
| R | 5.99% |
| D | 4.25% |
| L | 4.03% |
| C | 2.78% |
| U | 2.76% |
| M | 2.41% |
| W | 2.36% |
| F | 2.23% |
| G | 2.02% |
| Y | 1.97% |
| P | 1.93% |
| B | 1.49% |
| V | 0.98% |
| K | 0.77% |
| J | 0.15% |
| X | 0.15% |
| Q | 0.10% |
| Z | 0.07% |

[Return Back](#_Methodology)

### Statistic for Cipher Letter of Text

|  |  |  |  |
| --- | --- | --- | --- |
| Cipher Letter | Frequency | Frequency Rate | Corresponding Letter |
| U | 45x | 11.54% | E |
| Q | 32x | 8.21% | T |
| H | 32x | 8.21% | S |
| F | 28x | 7.18% | I |
| B | 25x | 6% | R |
| L | 25x | 6% | L |
| P | 23x | 5.9% | O |
| D | 23x | 5.9% | C |
| R | 20x | 5.13% | A |
| G | 19x | 4.87% | N |
| N | 16x | 4.1% | M |
| K | 15x | 3.85% | D |
| W | 14x | 3.59% | P |
| O | 13x | 3.33% | H |
| X | 13x | 3.33% | U |
| S | 12x | 3.08% | Y |
| E | 9x | 2.31% | G |
| I | 9x | 2.31% | B |
| V | 8x | 2.05% | K |
| C | 5x | 1.28% | W |
| T | 2x | 0.51% | V |
| Z | 1x | 0.26% | F |
| Y | 1x | 0.26% | Z |

[Return Back](#_Methodology)

### Graphic for Cipher Letters and Normal Letters (Appendix Page)

[Return Back](#_Methodology)

# Reference

|  |  |
| --- | --- |
| [1] | Indeed, “indded,” indeed, 2019. [Online]. Available: https://www.indeed.com/viewjob?jk=0b0710819e30ac94&tk=1doo6eoranvha801&from=serp&vjs=3. |
| [2] | T. DeGroat, “Springboard,” 18 7 2018. [Online]. Available: https://www.springboard.com/blog/cybersecurity-certifications/. |
| [3] | Payscale, “Payscale,” Payscale, 18 9 2019. [Online]. Available: https://www.payscale.com/research/AU/Job=Security\_Manager/Salary. |
| [4] | careerbuilder, “careerbuilder,” careerbuilder, 13 2 2019. [Online]. Available: https://www.careerbuilder.com/jobs?utf8=%E2%9C%93&keywords=Security+%2B+Certi%EF%AC%81cation&location=Australia. |
| [5] | E. R. Tauchman, “CompTia,” CompTia, 10 Aug 2018. [Online]. Available: https://www.comptia.org/blog/the-top-9-jobs-in-cybersecurity. |
| [6] | I. Resources, “ Infosec Resources,” Infosec Resources, 30 Dec 2018. [Online]. Available: https://resources.infosecinstitute.com/average-cissp-salary-2013/#gref. |
| [7] | I. Resources, “ Infosec Resources,” Infosec Resources, 25 Oct. 2018. [Online]. Available: https://resources.infosecinstitute.com/category/cybersecurity-careers/how-to-become-a-cybersecurity-analyst/cybersecurity-analyst-job-description/#gref. |
| [8] | D. Brecht, “Security+ Certification,” Infosec Resources , 30 Aug 2017. [Online]. Available: https://resources.infosecinstitute.com/category/cybersecurity-careers/how-to-become-a-cybersecurity-analyst/#gref. |
| [9] | D. Rijmenants, “CIPHER MACHINES AND CRYPTOLOGY,” 2019. [Online]. Available: http://users.telenet.be/d.rijmenants/en/onetimepad.htm. |
| [10] | L. V. Niekerk, “iTouch News,” iTouch News, 2019. [Online]. Available: https://itouch.co.za/news/10-uses-otp.php. |
| [11] | B. Mitchell, “Should you bring your own device to work?,” LifeWire, 10 Jun. 2019. [Online]. Available: https://www.lifewire.com/an-introduction-to-byod-for-it-networks-817819. |
| [12] | M. P. &. P. SCIENCES, “BYOD-Guidelines-2019w,” 2019. [Online]. Available: https://www.monash.edu/\_\_data/assets/pdf\_file/0007/1368529/BYOD-Guidelines-2019web.pdf. |
| [13] | A. Thompson, “Writing the Next Chapter for the Historic One-Time Pad,” 4 5 2016. [Online]. Available: http://www.circleid.com/posts/20160504\_writing\_the\_next\_chapter\_for\_the\_historic\_one\_time\_pad/. |
| [14] | Payscale, 2018. [Online]. Available: https://www.payscale.com/research/US/Job=Network\_Engineer/Salary. |
| [15] | UB, UniversityBusiness, 1 Nov. 2018. [Online]. Available: https://universitybusiness.co.uk/Article/building-byod/. |
| [16] | Roger A. Grimes, Josh Fruhlinger, “What is OAuth? How the open authorization framework works,” CSO, 20 Sep. 2019. [Online]. Available: https://www.csoonline.com/article/3216404/what-is-oauth-how-the-open-authorization-framework-works.html. |
| [17] | Microsoft, “ The OAuth 2.0 Authorization Framework,” Oct 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749#page-4. |
| [18] | A. A, “The Pros and Cons of using Authentication,” Habile, 27 June 2017. [Online]. Available: https://habiletechnologies.com/blog/pros-cons-using-authentication/. |
| [19] | Jim, “OAuth 2.0 Vulnerabilities,” Idapwiki, 15 Aug 2019. [Online]. Available: https://ldapwiki.com/wiki/OAuth%202.0%20Vulnerabilities. |
| [20] | PayScale, “Average Cyber Security Analyst Salary,” 2018. [Online]. Available: https://www.payscale.com/research/US/Job=Cyber\_Security\_Analyst/Salary. |
| [21] | Payscale, “CompTIA Security+ Salary | PayScale,” 2018. [Online]. Available: https://www.payscale.com/research/US/Certification=CompTIA\_Security%2B/Salary . |
| [22] | “Average Information Technology (IT) Manager Salary,” 2018. [Online]. Available: https://www.payscale.com/research/US/Job=Information\_Technology\_(IT)\_Manager/Salary. |
| [23] | R. A. Grimes, “What is OAuth? How the open authorization framework works,” 2017. [Online]. Available: https://www.csoonline.com/article/3216404/authentication/what-is-oauth-how-the-open-authorization-framework-works.html. |
| [24] | L. V. Niekerk, “iTouch News,” iTouch, 2019. [Online]. Available: https://itouch.co.za/news/10-uses-otp.php. |
| [25] | David Wiershem, Guoying Zhang, Charles R. Johnston, “Journal of International Technology and Information Management,” Texas, 2010. |
| [26] | A. Berthene, “Internet Retailer,” DigitalCommerce, 26 Oct 2017. [Online]. Available: https://www.digitalcommerce360.com/2017/10/26/mobile-devices-will-account-73-internet-consumption-in-2018/. |
| [27] | M. Rouse, “virtual desktop infrastructure (VDI),” TechTarget, Jan. 2017. [Online]. Available: https://searchvirtualdesktop.techtarget.com/definition/virtual-desktop-infrastructure-VDI. |