| Office Use Only |
| --- |
| ☐ Assignment Received |
| ☐ Before due date & time |
| ☐ Late Submission |

| | |
| --- | --- |
| **PROGRAMME** | DIPLOMA TEKNOLOGI MAKLUMAT (DTM) |
| **SUBJECT CODE & NAME** | KCT1223 COMPUTER AND NETWORK SECURITY. |
| **TUTOR NAME** | PUAN NUR ALYANI MOHD NOR |
| **ASSIGNMENT TITLE** | ASSIGMENT 1 |

Please note that it is your responsibility to retain copies of your assignment. Copying someone else's work is plagiarism, and is unacceptable. The college may impose severe penalties for plagiarism. All work must be submitted by the due date. If an extension of work is granted, this must be specified with the signature of the lecturer/tutor.

**GROUP ASSIGNMENT**

| STUDENT NAME | MATRIX NUMBER | SIGNATURE |
| --- | --- | --- |
| VHETHAASHINI A/P THANGARAJU | 1052023070024 | *VHETHAA* |

**OFFICE USE ONLY**

| | |
| --- | --- |
| Tutor Name | PUAN NUR ALYANI MOHD NOR |
| Marking Comment & Feedback | |
| Result/Grade | |

# Isi Kandungan

## 1.0 PENGENALAN

Dalam era digital yang semakin berkembang pesat, isu keselamatan siber menjadi semakin penting. Maklumat peribadi, kewangan, dan organisasi kini berada dalam ancaman jenayah siber yang berasaskan kepada kod berniat jahat (malicious code). Oleh itu, konsep kriptografi seperti cipher dan enkripsi digunakan untuk melindungi komunikasi dan data sensitif.

Menurut CyberSecurity Malaysia, jenayah siber meningkat 22% setiap tahun. Serangan berasaskan kod berniat jahat seperti ransomware dan spyware menyebabkan kerugian berjuta ringgit setiap tahun. Justeru itu, kesedaran terhadap kriptografi dan enkripsi adalah penting dalam menangani isu ini.

Laporan ini akan menghuraikan tiga aspek penting: jenis cipher, jenayah siber berkaitan malicious code, dan proses enkripsi menggunakan public dan private key.

## 2.0 CIPHER – SHIFT CIPHER

Cipher merupakan teknik dalam kriptografi yang digunakan untuk menyulitkan mesej agar hanya penerima yang mempunyai kunci penyahsulitan dapat memahaminya. Salah satu cipher yang paling awal dan terkenal ialah Shift Cipher, atau lebih dikenali sebagai Caesar Cipher. Teknik ini melibatkan penggantian setiap huruf dalam mesej asal dengan huruf lain berdasarkan peralihan tertentu dalam abjad.

### 2.1 Definisi Cipher

Cipher ialah kaedah menyulitkan mesej supaya kandungannya tidak dapat difahami oleh pihak yang tidak dibenarkan. Cipher digunakan sejak zaman dahulu dalam komunikasi rahsia dan kini diaplikasikan secara moden dalam pelbagai sistem keselamatan digital.

### 2.2 Shift Cipher (Caesar Cipher)

Shift Cipher, atau Caesar Cipher, merupakan teknik cipher klasik yang menyusun semula huruf dalam mesej asal berdasarkan nilai peralihan tertentu. Contohnya, jika mesej asal ialah “HELLO” dan peralihan sebanyak +3 digunakan, hasil mesej yang disulitkan ialah “KHOOR”.

- Contoh:

➢ Mesej asal: HELLO

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

➢ Guna shift +3: H → K, E → H, L → O, O → R

➢ Mesej disulitkan: KHOOR

## 2.3 Aplikasi Shift Cipher

Shift Cipher sering digunakan dalam pelbagai situasi yang memerlukan penyulitan data yang mudah, seperti dalam permainan teka-teki atau sistem pengesahan yang tidak melibatkan maklumat sensitif. Kadang-kadang, Shift Cipher juga digunakan dalam sistem CAPTCHA untuk memastikan bahawa hanya pengguna manusia yang boleh mengakses laman web atau aplikasi tertentu. Walau bagaimanapun, penggunaannya dalam situasi yang lebih kritikal adalah sangat terhad kerana kelemahannya dalam keselamatan.

## 2.4 Kelebihan dan Kelemahan

Shift Cipher mempunyai beberapa kelebihan yang menjadikannya sesuai digunakan dalam konteks tertentu. Antaranya ialah teknik ini sangat mudah difahami dan diaplikasikan, terutama oleh mereka yang baru belajar asas kriptografi. Ia juga sesuai digunakan dalam situasi yang tidak kritikal seperti permainan teka-teki atau aktiviti pembelajaran asas penyulitan kerana pendekatannya yang ringkas dan tidak memerlukan pemahaman teknikal yang mendalam.

Namun begitu, Shift Cipher juga mempunyai kelemahan yang ketara. Tahap keselamatan teknik ini adalah sangat rendah kerana ia hanya mempunyai 25 kemungkinan peralihan huruf yang sah, menjadikannya mudah untuk dipecahkan dengan kaedah brute-force. Dalam serangan sebegini, penyerang hanya perlu mencuba setiap kemungkinan peralihan sehingga mesej asal berjaya didedahkan. Oleh sebab itu, penggunaan Shift Cipher tidak digalakkan dalam situasi yang memerlukan keselamatan data yang tinggi.

## 3.0 JENAYAH SIBER BERKAITAN KOD BERNIAT JAHAT (MALICIOUS CODE)

### 3.1 Definisi Jenayah Siber

Jenayah siber merujuk kepada sebarang jenayah yang berlaku melalui rangkaian komputer atau internet. Aktiviti jenayah ini sering melibatkan penggunaan kod berniat jahat yang bertujuan untuk mencuri data, merosakkan sistem, atau menipu pengguna. Kod berniat jahat ini boleh mengakibatkan kerugian besar, sama ada dalam bentuk kerosakan sistem atau kehilangan maklumat peribadi yang sangat bernilai. Antara jenis-jenis kod berniat jahat yang sering digunakan dalam jenayah siber adalah virus, worms, trojan horse, spyware, dan ransomware.

### 3.2 Jenis-jenis Kod Berniat Jahat

Virus adalah salah satu jenis kod berniat jahat yang menjangkiti fail dan perisian dalam sistem komputer. Virus ini diaktifkan apabila pengguna membuka fail yang dijangkiti. Sebagai contoh, virus boleh tersebar melalui pemacu USB yang mengubah fail tugasan menjadi fail berformat .exe. Virus ini biasanya menyebabkan sistem komputer menjadi perlahan atau rosak, dan dalam kes yang lebih teruk, ia boleh menghapuskan data yang disimpan dalam sistem.

Worms pula adalah kod berniat jahat yang berbeza kerana ia dapat merebak sendiri melalui rangkaian tanpa memerlukan tindakan daripada pengguna. Worms ini boleh menyerang komputer-komputer lain dalam rangkaian dengan mengeksploitasi kelemahan dalam sistem, menyebabkan gangguan besar kepada operasi rangkaian. Contohnya adalah serangan Slammer Worm yang menyerang server syarikat, menyebabkan sistem mereka menjadi tidak dapat digunakan dan mempengaruhi sistem lain dalam rangkaian.

Trojan Horse adalah jenis kod berniat jahat yang menyamar sebagai program yang kelihatan sah atau berguna, tetapi sebenarnya mengandungi kod merbahaya. Contohnya, permainan percuma palsu yang dimuat turun dari laman web tidak sah boleh memasukkan virus ke dalam sistem komputer pengguna, membenarkan penjenayah siber mengakses data atau merosakkan sistem tanpa disedari oleh pengguna.

Spyware pula bertindak untuk mengintip aktiviti pengguna dan mencuri maklumat peribadi seperti kata laluan, nombor kad kredit, dan data sensitif lainnya. Spyware ini biasanya tersembunyi dalam aplikasi atau extension yang dimuat turun tanpa pengetahuan pengguna. Sebagai contoh, extension Chrome palsu yang menyalin data login pengguna tanpa mereka sedari boleh menyebabkan pencerobohan privasi yang serius.

Ransomware adalah salah satu jenis kod berniat jahat yang paling merosakkan. Ia berfungsi dengan mengunci fail penting dalam sistem dan meminta wang tebusan untuk membukanya semula. Serangan WannaCry yang menyasarkan hospital dan pejabat kerajaan adalah contoh serangan ransomware yang besar, di mana penjenayah siber menuntut bayaran dalam bentuk mata wang digital untuk membuka semula akses kepada fail yang terkunci.

### 3.3 Langkah Pencegahan

Untuk mencegah serangan jenayah siber yang melibatkan kod berniat jahat, langkah-langkah pencegahan yang betul harus diambil. Antaranya adalah sentiasa memastikan antivirus terkini dipasang dan dikemas kini secara berkala untuk mengesan dan menghapuskan kod berniat jahat. Selain itu, pengguna juga harus berhati-hati dan mengelakkan mengklik pautan yang mencurigakan atau memuat turun fail dari laman web yang tidak sah, kerana ini merupakan salah satu cara utama penyebaran kod berniat jahat. Menggunakan firewall yang kuat juga penting untuk melindungi rangkaian daripada ancaman luar, dan memastikan sistem sandaran data dilaksanakan secara berkala agar data penting boleh dipulihkan sekiranya berlaku serangan.

## 4.0 ENKRIPSI PUBLIC DAN PRIVATE KEY

### 4.1 Definisi Enkripsi

Enkripsi ialah proses menukar data biasa kepada bentuk rahsia supaya tidak boleh difahami oleh pihak tidak dibenarkan. Ia membantu dalam menjamin kerahsiaan dan keselamatan komunikasi.

### 4.2 Jenis Enkripsi

Enkripsi terbahagi kepada dua jenis utama: Symmetric Encryption dan Asymmetric Encryption.

Symmetric Encryption menggunakan satu kunci yang sama untuk menyulitkan dan menyahsulit data. Proses ini adalah lebih cepat dan lebih mudah dilaksanakan, namun, terdapat kelemahan utama iaitu jika kunci tersebut diketahui oleh pihak luar, maka keseluruhan sistem enkripsi boleh terdedah.

Sementara itu, Asymmetric Encryption menggunakan dua kunci yang berbeza, iaitu public key dan private key. Public key digunakan untuk menyulitkan mesej, manakala private key digunakan untuk menyahsulitkan mesej tersebut. Jenis enkripsi ini lebih selamat kerana hanya pemilik private key yang dapat menyahsulit mesej yang disulitkan dengan public key. Ini menjadikan enkripsi jenis ini lebih selamat, terutama dalam situasi di mana kunci perlu dikongsi melalui saluran yang tidak selamat.

## 4.3 Mekanisme Asymmetric Encryption

Dalam sistem enkripsi asymmetric, public key digunakan untuk menyulitkan mesej yang dihantar oleh penghantar. Setelah mesej disulitkan dengan public key, hanya penerima yang memiliki private key yang sesuai boleh menyahsulit mesej tersebut. Dengan cara ini, meskipun public key boleh dikongsi secara terbuka, hanya penerima yang sah yang dapat membaca mesej tersebut dengan menggunakan private key mereka. Sistem ini menjamin keselamatan komunikasi, kerana private key tidak perlu dikongsi dengan sesiapa.

## 4.4 Situasi Penggunaan:Ali & Raju

Sebagai contoh, katakan Ali ingin menghantar mesej rahsia kepada Raju. Ali akan menggunakan public key milik Raju untuk menyulitkan mesej tersebut. Setelah mesej dihantar, Raju, yang memiliki private key miliknya, akan menyahsulitkan mesej tersebut. Dengan cara ini, walaupun mesej itu dihantar melalui saluran yang mungkin tidak selamat, hanya Raju yang dapat membacanya kerana hanya dia yang memiliki private key untuk menyahsulit mesej tersebut.

## 4.5 Contoh Teknik

Beberapa contoh teknik enkripsi public dan private key termasuk RSA, ElGamal, ECC (Elliptic Curve Cryptography), dan DSA (Digital Signature Algorithm). Teknik-teknik ini digunakan dalam pelbagai aplikasi, seperti e-mel selamat, perbankan dalam talian, dan HTTPS di laman web. Penggunaan teknik ini membolehkan pengguna berkomunikasi dengan lebih selamat di persekitaran digital yang terdedah kepada ancaman luar.

4.6 Jadual Perbandingan

| Jenis Enkripsi | Kunci Digunakan | Kelebihan | Contoh |
|---|---|---|---|
| Symmetric | 1 kunci sahaja | "Cepat dan ringan, sesuai untuk penggunaan dengan data yang besar dan dalam persekitaran yang memerlukan kecekapan tinggi. Namun, jika kunci diketahui pihak luar, keselamatannya terjejas." | AES, DES |
| Asymmetric | Public & Private Key | Lebih selamat kerana menggunakan dua kunci yang berbeza, di mana public key boleh dikongsi secara terbuka, tetapi hanya pemegang private key yang dapat menyahsulitkan data. Sesuai untuk komunikasi jarak jauh atau persekitaran tidak selamat. | RSA, ECC, ElGamal |

Penjelasan Jadual:
*Symmetric Encryption:*

Kunci Digunakan adalah hanya satu kunci yang digunakan untuk kedua-dua proses penyulitan (enkripsi) dan penyahsulitan (dekripsi).

Kelebihan adalah proses enkripsi dan penyahsulitan lebih cepat kerana hanya satu kunci yang digunakan. Ia sangat berguna apabila data yang dihantar besar dan memerlukan kecekapan tinggi. Walau bagaimanapun, apabila kunci ini diketahui pihak luar, keselamatannya akan terjejas kerana sesiapa sahaja yang mempunyai kunci tersebut boleh menyulitkan dan menyahsulitkan data.

Contohnya adalah AES (Advanced Encryption Standard) dan DES (Data Encryption Standard) adalah dua contoh teknik enkripsi simetrik yang sering digunakan.

*Asymmetric Encryption:*

Kunci Digunakan ialah menggunakan dua kunci berbeza, iaitu public key dan private key. Public key boleh dikongsi secara terbuka, sementara private key disimpan secara rahsia oleh penerima.

Kelebihan adalah dengan dua kunci yang berbeza, keselamatan meningkat kerana kunci yang digunakan untuk menyulitkan mesej (public key) berbeza daripada kunci yang digunakan untuk menyahsulitkan mesej (private key). Oleh itu, walaupun public key didedahkan kepada orang ramai, hanya pemegang private key yang sah boleh menyahsulitkan data tersebut. Teknik ini lebih sesuai untuk komunikasi dalam persekitaran tidak selamat atau apabila penghantaran data perlu dilakukan jarak jauh.

Contohnya adalah RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), dan ElGamal adalah beberapa contoh algoritma enkripsi tidak simetrik yang biasa digunakan.

## 5.0 KESIMPULAN

Kriptografi memainkan peranan yang sangat penting dalam menjaga keselamatan siber, di mana teknik seperti cipher digunakan untuk menyulitkan maklumat agar tidak mudah diakses oleh pihak yang tidak dibenarkan. Contoh yang terkenal adalah Shift Cipher yang mengubah setiap huruf dalam mesej asal berdasarkan peralihan tertentu, memberi asas kepada konsep keselamatan maklumat yang lebih kompleks. Namun, selain teknik penyulitan, penting juga untuk kita memahami pelbagai bentuk jenayah siber yang berkaitan dengan kod berniat jahat. Jenayah seperti virus, worms, trojan horse, spyware, dan ransomware sering digunakan oleh penjenayah siber untuk mencuri data, merosakkan sistem, atau memeras wang dari mangsa. Oleh itu, pemahaman yang baik tentang jenis-jenis kod berniat jahat ini sangat penting untuk langkah pencegahan yang betul, termasuk penggunaan perisian antivirus yang terkini dan mengelakkan membuka pautan atau fail yang mencurigakan.

Selain itu, penggunaan enkripsi dengan kunci awam dan kunci peribadi (public key dan private key) memberikan perlindungan yang lebih kukuh dalam komunikasi digital. Berbanding dengan enkripsi simetrik yang hanya menggunakan satu kunci, teknik ini menawarkan keselamatan yang lebih tinggi kerana kunci peribadi tidak dikongsi antara pihak yang terlibat. Public key digunakan untuk menyulitkan mesej, manakala private key digunakan untuk menyahsulitkan mesej tersebut. Teknik enkripsi ini digunakan dalam aplikasi seperti perbankan dalam talian dan e-dokumen rasmi, menjadikannya amat penting dalam memastikan keselamatan dan kerahsiaan maklumat. Dengan kesedaran yang lebih tinggi tentang amalan keselamatan siber, kita dapat melindungi diri daripada ancaman yang semakin berkembang dalam dunia digital yang semakin canggih.

Rujukan:


- https://www.kaspersky.com/resource-center/threats/malware
- https://www.techtarget.com/searchsecurity/definition/encryption
- https://www.youtube.com/watch?v=EKUu0aWyhpM
- https://www.youtube.com/watch?v=fpE6gWeZyfE
- https://www.youtube.com/watch?v=lsbYqJXB2es
- https://www.youtube.com/watch?v=lsbYqJXB2es
- https://www.youtube.com/watch?v=eKZT35Di9Lg