BLOCKCHAIN NOVEMBER 21, 2018 14:01

Kriptografi: Sejarah Dan Asal Usulnya

Penulis: Dr. Muhammad Reza bin Z'aba, Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Malaya

Sejak Bitcoin menjadi popular dalam 2 tahun kebelakangan ini, perkataan kriptografi semakin sering didengar. Malah, apabila disebut "kripto", orang awam akan terus mengaitkannya dengan mata wang kripto. Namun, apakah itu kriptografi? Daripada mana asal-usulnya? Artikel ini berhasrat untuk merungkai persoalan ini.

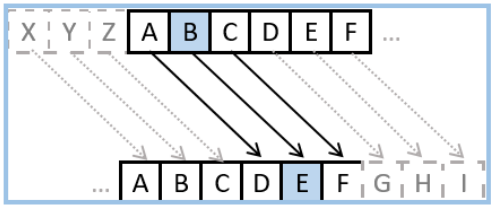
Perkataan **kriptografi** ni berasal daripada dua istilah Yunani (Greek) lama iaitu "kryptos" dan "graphein". "Kryptos" bermaksud 'rahsia' manakala "graphein" membawa makna 'menulis'. Jadi, kalau kita gabung kedua-dua perkataan ini dapatlah perkataan "tulisan rahsia". Satu lagi istilah yang berkaitan ialah **steganografi**, juga berasal daripada istilah Yunani lama "steganos" yang bermaksud 'menyembunyikan'.

Kriptografi akan mengubah mesej asal manakala steganografi tidak mengubah mesej asal, tetapi menyembunyikannya dalam satu medium yang lain. Dalam artikel ini, steganografi dianggap sebahagian daripada kriptografi.

Penggunaan kriptografi boleh dijejak seawal kurun ke-5 sebelum Masihi (SM), iaitu semasa pertembungan antara empayar Yunani dan Parsi. Pada waktu itu, sebuah **tablet kayu** yang telah dikikis lilinnya, telah digunakan untuk menulis mesej rahsia. Kemudian, mesej tersebut dilapiskan semula dengan lilin sehingga pada luarannya, kelihatan seolah-olah tiada apa-apa mesej yang tertulis di tablet tersebut. Untuk merungkai mesej asal, lilin luaran pada tablet kayu tersebut perlu dikikis untuk mendedahkan mesej rahsia.

Cipher (sifer)

Kemudian, pada kurun pertama sebelum Masihi, Julius Caesar telah menggunakan suatu teknik kriptografi yang menggantikan setiap huruf dengan huruf ketiga selepasnya. Misalnya, perkataan “kripto” ditukar menjadi “mulswr”. Teknik ini kini dikenali sebagai **sifer Caesar** dan menjadi asas kepada sifer penggantian (**subsitution cipher**).



SHIFT +3

This Caesar cipher has a shift of 3 characters.

The letter 'A' becomes a 'D'. The letter 'B' becomes 'E'.

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

Sifer-sifer lain yang melibatkan manipulasi huruf termasuklah **transposisi** dan **Vigenère**. Semua sifer ini boleh diklasifikasikan sebagai sifer klasik kerana hanya melibatkan huruf dan sudah tidak lagi selamat digunakan kini. Namun, prinsip-prinsip asas dalam sifer-sifer klasik ini masih digunakan dalam sifer-sifer moden.

Dalam isitilah kriptografi, maklumat asal dipanggil **teks-biasa** (plaintext) manakala maklumat yang telah diubah dinamakan **teks-sifer** (ciphertext). Penamaan ini terpakai walaupun teks-biasa tersebut ialah maklumat digital lain seperti gambar, video dan audio. Proses penukaran teks-asal ke teks-sifer dipanggil "**enkripsi**", manakala proses sebaliknya ialah "dekripsi".

Perkembangan kriptanalisis

Pada kurun ke-9, seorang sarjana Muslim bernama **Abu Yusuf Ya'qub ibn Ishaq as-Sabbah al-Khindi** telah menjadi individu pertama yang melakukan kajian dalam ilmu **kriptanalisis**, iaitu tentang bagaimana menggodam atau memecahkan kriptografi. Dalam bukunya, "Risala fi Istikhraj al-Kutub al-Mu'amah" (literal: Manuskrip tentang Mentafsirkan Mesej yang Disembunyikan), beliau menerangkan tentang kaedah **analisa frekuensi** untuk mentafsirkan teks-sifer yang dilindungi menggunakan sifer penggantian. Contohnya, dalam bahasa Inggeris, secara purata, 'e' merupakan huruf yang paling banyak digunakan dalam suatu teks. Justeru, jika suatu teks-sifer didapati mengandungi banyak huruf 'g', kemungkinan besar huruf 'g' tersebut ialah huruf 'e' dalam teks-biasa.

Dalam kurun-kurun berikutnya, kriptografi berasaskan huruf masih terus digunakan. Dalam masa yang sama, ilmu kriptanalisis juga berkembang. Pada hujung kurun ke-19, **Steve Babbage**, yang digelar "Bapa Komputer", dan **Friedrich Kasiski**, secara berasingan telah berjaya mematahkan sifer **Vigenère**. Kemajuan dalam ilmu kriptanalisis telah memaksa ahli kriptografi untuk mencipta sifer baru yang lebih selamat.

OTP

Sekitar penghujung tahun 1910an, **Mejar Joseph Mauborgne**, Ketua Penyelidikan Kriptografi untuk tentera Amerika Syarikat (AS), telah menemukan teknik **one-time-pad** (OTP). Ciri-ciri utama OTP ialah kekunci rahsia perlu dijana secara rawak, panjang kekunci mesti sama dengan mesej, dan kekunci hanya boleh digunakan sekali dan tidak boleh diguna semula untuk enkrip mesej yang lain. Disebabkan ciri-ciri ini, masalah-masalah lain timbul. Bagaimana untuk mendapatkan sumber rawak yang baik? Bagaimana untuk berkongsi kekunci rahsia yang panjang secara selamat dan cepat? Justeru, OTP tidak praktikal untuk digunapakai, terutama semasa perang, dimana mesej perlu dihantar segera.

Enigma

Kredit : BT.com

Pada tahun 1918, **Arthur Scherbius**, seorang jurutera elektrik Jerman, telah mencipta sebuah mesin sifer mekanikal yang dipanggil **Enigma**. Terdapat pelbagai variasi Enigma dihasilkan dan telah digunakan oleh pelbagai pihak terutama tentera Nazi Jerman semasa Perang Dunia Kedua (1939-1945). Pada tahun 1932, **Marian Rejewski**, seorang ahli matematik di Biro Sifer Poland, bersama-sama pasukannya, telah berjaya menggodam satu variasi Enigma yang digunakan oleh pihak tentera Nazi Jerman. Pada tahun 1939, pihak Jerman telah meningkatkan ciri-ciri keselamatan Enigma, dan usaha untuk menggodam Enigma telah menjadi lebih sukar.

Selepas Jerman menceroboh Poland pada 1 September 1939, usaha-usaha menggodam Enigma diteruskan oleh ahli-ahli kriptanalisis British di **Bletchley Park**. Antara kejayaan paling besar ialah daripada ahli matematik **Alan Turing**. Pada 1940, beliau telah berjaya mencipta mesin untuk

melakukan kriptanalisis ke atas Enigma yang akhirnya membantu pihak Bersekutu untuk menamatkan Perang Dunia ke-2 pada tahun 1945.

Kalau kita lihat, daripada kurun ke-5 sebelum Masihi sehinggalah pertengahan kurun ke-20, iaitu lebih kurang selama 2400 tahun, penggunaan kriptografi adalah tertumpu kepada usaha melindungi maklumat rahsia daripada pihak yang tidak berkenaan. Kini, kriptografi telah diperluaskan takrifannya dan merangkumi kajian tentang teknik-teknik keselamatan dalam melindungi bukan sahaja **kerahsiaan, tetapi juga integriti, keaslian, dan ketidaksangkalan maklumat**.

Kriptografi di zaman Moden

Pada tahun 1976, **Whitfield Diffie** dan **Martin Hellman** daripada Universiti Stanford telah memperkenalkan **konsep-konsep awal** dalam mewujudkan **kriptografi kekunci awam** dan **tandatangan digital**. Ini termasuk keperluan untuk membina **hash function** yang berfungsi untuk memastikan integriti maklumat terjaga. Antara algoritma hash function terawal yang dibina ialah **MD2** oleh **Ronald Rivest** pada tahun 1989. Algoritma hash function popular yang digunakan oleh mata wang kripto kini ialah **SHA-256**, yang dicipta oleh **National Security Agency (NSA)** AS pada tahun 2001.

Antara algoritma awal tandatangan digital, yang memberikan ciri **ketidaksangkalan**, ialah **RSA** yang dicipta oleh **Ronald Rivest**, **Adi Shamir** dan **Leonard Adleman** pada tahun 1978. Algoritma yang sering digunakan dalam mata wang kripto ialah **Elliptic Curve Digital Signature Algorithm (ECDSA)**, yang dicadangkan oleh **Scott Vanstone** pada tahun 1992. ECDSA merupakan versi **kriptografi elliptic curve** bagi **Digital Signature Algorithm (DSA)** yang diterbitkan oleh **National Institute of Standards and Technology (NIST)** AS pada tahun 1991.

Penggunaan kriptografi pada zaman ini amat meluas. Boleh dikatakan bahawa, tanpa kriptografi, adalah mustahil untuk melakukan sesuatu transaksi dengan selamat di alam maya. Dalam artikel-artikel akan datang, kita akan melihat lebih dekat tentang hash function dan tandatangan digital.

Nota:

Maklumat tentang sejarah awal kriptografi adalah bersumberkan buku "**The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography**" karangan **Simon Singh**. Buku lain yang popular ialah tulisan **David Khan**yang berjudul "**The Codebreakers: The Comprehensive History of Secret Communcation from Ancient Times to the Internet**".

BLOCKCHAIN | BLOCKCHAIN TECHNOLOGY | TEKNOLOGI BLOCKCHAIN

Dr. Muhammad Reza Bin Z'aba

REGULATION NOVEMBER 26, 2018 19:53

Teknologi Blockchain: Adakah Malaysia Bersedia?

TEKNOLOGI BLOCKCHAIN: ADAKAH MALAYSIA BERSEDIA?

Baru-baru ini, kecoh media sosial dengan cemuhan dan kritikan terhadap Harapan Coin, sebuah inisiatif YB Khalid Samad dalam menyediakan dana untuk Pakatan Harapan berhadapan dengan PRU14 tempoh hari. Semuanya gara-gara sikap segilintir pihak media yang memetik kata-kata YB