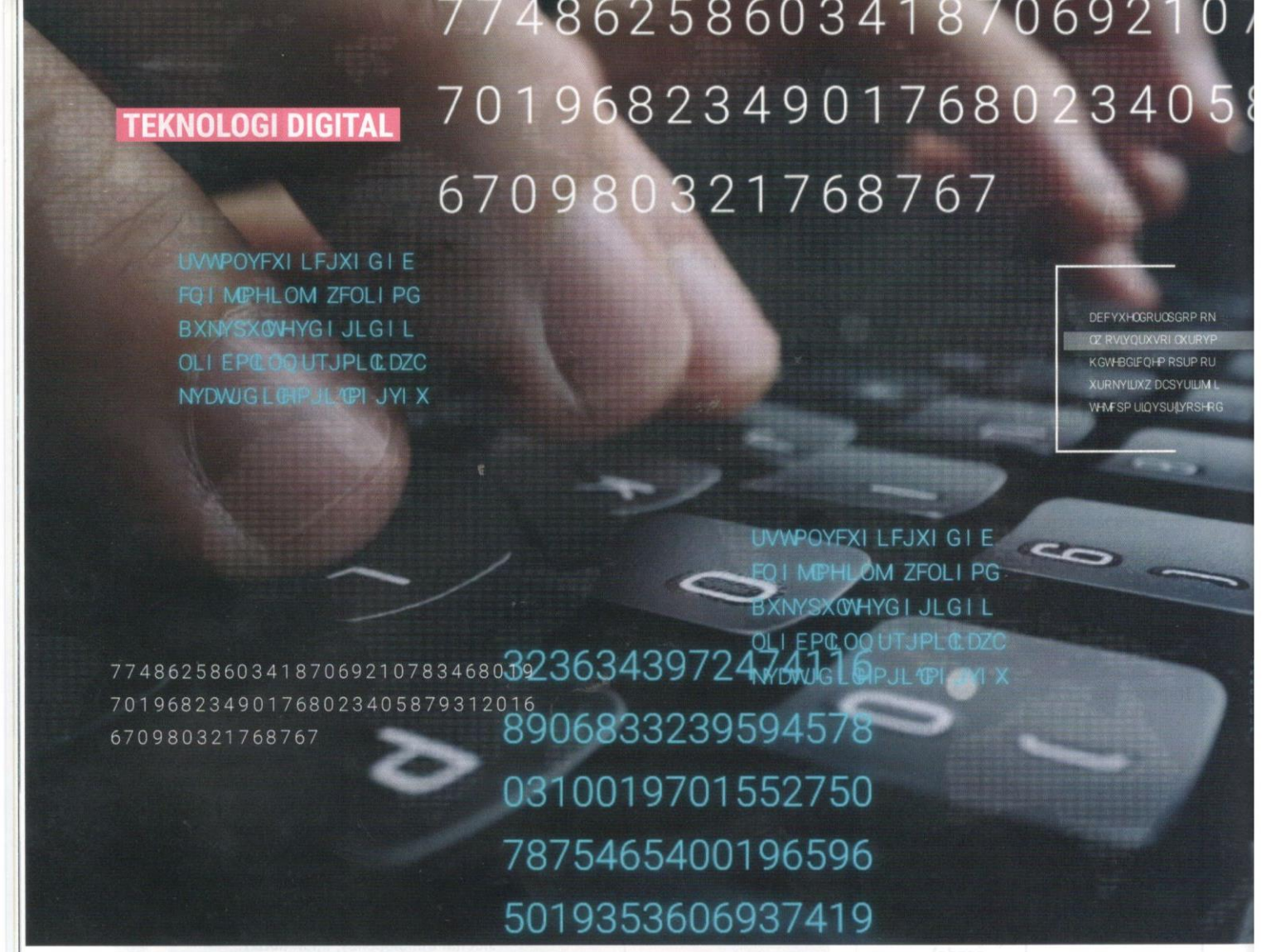


Kriptografi sebagai Kunci Keselamatan Teknologi Digital

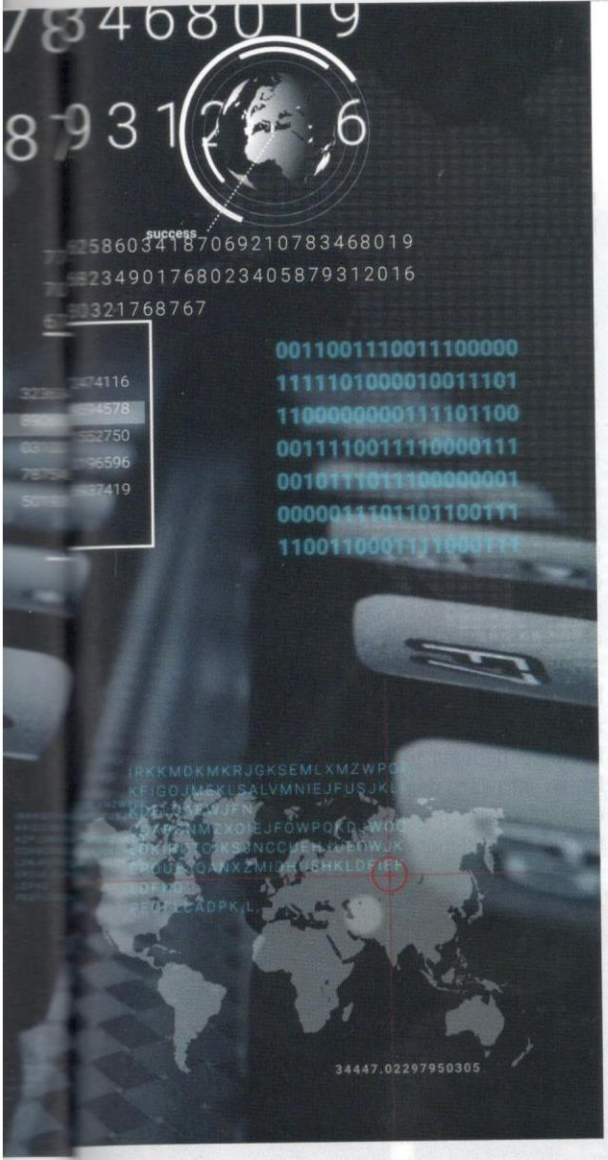
Amir Hamzah Abd Ghafar

Kerahsiaan ialah elemen penting sejak manusia mula bersaing antara satu sama lain. Dalam sejarah awal manusia, kejayaan menyembunyikan rahsia dalam perniagaan, peperangan, politik, dan teknologi daripada pengetahuan musuh menjadi tunjang penting dalam melonjakkan suatu sistem ketamadunan mengatasi ketamadunan yang lain. Kejayaan ini dicapai dengan menggunakan suatu teknik yang dipanggil sebagai kriptografi.

Perkataan kriptografi berasal daripada perkataan Greek kuno, iaitu *kryptós* yang bermaksud "merahsiakan" serta *graphein*, "untuk menulis". Maka, teknik kriptografi dapat dijelaskan sebagai teknik menulis untuk merahsiakan sesuatu.

Secara umumnya, kriptografi digunakan untuk mengubah suatu perkataan yang dipanggil sebagai teks asal kepada suatu perkataan yang tidak membawa apa-apa maksud yang dikenali sebagai teks terubah selamat. Proses ini dipanggil sebagai penyulitan dan dilakukan oleh pihak yang ingin menghantar suatu maklumat.

Teks terubah selamat ini kemudiannya dihantar kepada penerima yang akan mengubah semula teks yang diterimanya kepada teks asal untuk dibaca. Proses ini dipanggil sebagai penyahsulitan. Kedua-dua proses ini akan berjaya dilakukan jika penghantar dan penerima teks terubah selamat itu berkongsi suatu kunci rahsia yang sama. Sekiranya musuh berjaya memintas suatu teks terubah selamat sebelum sampai kepada penerima, maklumat dalam teks asal tetap terpelihara kerana musuh tidak dapat melakukan proses penyahsulitan tanpa memiliki kunci rahsia.



Sistem kunci penyulitan dan penyahsulitan yang sama ini dipanggil sebagai kriptografi kunci simetrik atau kriptografi kunci rahsia. Sistem ini meliputi kesemua teknik kriptografi yang diamalkan sebelum abad ke-20. Alatan terawal kriptografi yang diketahui adalah suatu kayu khas yang dipanggil sebagai *scytale*. Alatan ini diperkenalkan dalam era Greek kuno dan penghantar serta penerima maklumat akan berkongsi *scytale* yang sama (atau hampir sama) untuk melakukan proses penyulitan dan penyahsulitan. Antara teknik kriptografi yang popular selepas itu ialah sifer caesar, bersempena dengan nama pemimpin Rom, Julius Caesar yang menggunakan teknik ini dalam kempen peperangannya.

Sejak sela masa tersebut, terdapat beberapa lagi teknik kriptografi kunci rahsia diperkenalkan seiring dengan perubahan teknologi ke arah mekanikal dan seterusnya elektromekanikal pada abad ke-20.

Skim pertukaran kunci Diffie-Hellman memanfaatkan suatu permasalahan sukar matematik yang dipanggil sebagai masalah logaritma diskrit bagi menjamin kerahsiaan kunci yang dikongsi oleh dua entiti.

Kemuncaknya, teknik kriptografi kunci rahsia seperti mesin penyulitan Enigma yang digunakan oleh kapal selam tentera Jerman dalam Perang Dunia Kedua mampu menggunakan kira-kira 16 900 jenis kunci yang boleh dikongsikan sesama mereka.

Selepas Perang Dunia Kedua tamat, keperluan untuk menyalurkan maklumat secara rahsia semakin meningkat sejajar dengan pertumbuhan rangkaian komunikasi yang melalui proses komersialisasi yang pesat. Maka, hal ini menimbulkan masalah yang belum pernah dialami pada masa sebelumnya. Kerumitan masalah ini boleh dilihat melalui situasi tertentu.

Sebagai contohnya, jika terdapat x entiti yang perlu berinteraksi antara satu sama lain, maka sejumlah $(x(x-1))/2$ kunci unik diperlukan bagi memastikan rangkaian ini dapat berkomunikasi dengan selamat. Bayangkan, sebuah syarikat yang mempunyai lebih daripada 10 buah cawangan di seluruh dunia memerlukan kira-kira 45 kunci rahsia yang perlu diagihkan bagi memastikan komunikasi sulit perniagaan tidak diketahui oleh pesaingnya. Apakah yang akan terjadi sekiranya syarikat tersebut mempunyai 100 buah cawangan?

Hal seperti ini semestinya menimbulkan kekalutan logistik dan kos operasi yang tinggi kerana setiap kali suatu rahsia ingin disalurkan kepada pihak tertentu, kunci rahsia yang sama bagi menyulitkan dan menyahsulitkan maklumat tersebut perlu diagihkan dengan pantas dan efisien. Masalah ini dipanggil sebagai masalah pengagihan kunci dan menghantui pelbagai pihak hingga dekad 70-an.

Pada tahun 1976, matematikawan di Amerika Syarikat telah menemui suatu kaedah penghitungan matematik untuk menyelesaikan masalah pengagihan kunci. Berbanding dengan kriptografi kunci rahsia, kaedah baharu ini menggunakan dua jenis kunci, yakni kunci awam dan kunci rahsia. Kedua-dua kunci tersebut dihubungkan melalui persamaan matematik. Nilai kunci rahsia ini hanya diketahui oleh pemilik kunci tersebut, manakala nilai kunci awam perlu dikongsikan bersama-sama setiap entiti yang terlibat dalam komunikasi tersebut.

Kaedah ini menyelesaikan kompleksiti dalam masalah pengagihan kunci kerana perkongsian kunci awam ini perlu dibuat sekali sahaja bagi setiap siri komunikasi yang melibatkan entiti yang sama. Kaedah ini juga boleh dilakukan tanpa melibatkan kos yang tinggi. Hal ini kerana sistem pengagihan kunci awam tidak perlu dijamin kerahsiaannya berbanding dengan sistem pengagihan kunci rahsia. Kaedah ini dikenali sebagai skim pertukaran kunci Diffie-Hellman yang diambil bersempena dengan nama penemunya. Kaedah ini menjadi titik tolak kemunculan era kriptografi kunci asimetrik atau kriptografi kunci awam.

Skim pertukaran kunci Diffie-Hellman memanfaatkan suatu permasalahan sukar matematik yang dipanggil sebagai masalah logaritma diskrit bagi menjamin kerahsiaan kunci yang dikongsi oleh dua entiti. Walau bagaimanapun, kaedah ini tidak dapat menjamin kesahihan identiti entiti yang terlibat menggunakannya. Jika satu daripada entiti yang terlibat itu disamari, entiti yang ingin berkomunikasi dengannya tidak dapat mengesahkan sama ada "kunci awam" yang diperolehnya itu dihantar oleh entiti sebenar atau penyamarnya.

Sehubungan dengan itu, dua tahun selepas kemunculan skim pertukaran kunci Diffie-Hellman, saintis komputer di Massachusetts Institute of Technology memperkenalkan algoritma RSA. Nama RSA digunakan bersempena dengan nama

penciptanya, iaitu Ron Rivest, Adi Shamir dan Leonard Adleman. Sistem kripto ini bukan sahaja boleh menyulitkan maklumat, malah mampu mengesahkan maklumat tersebut datang daripada entiti yang sepatutnya.

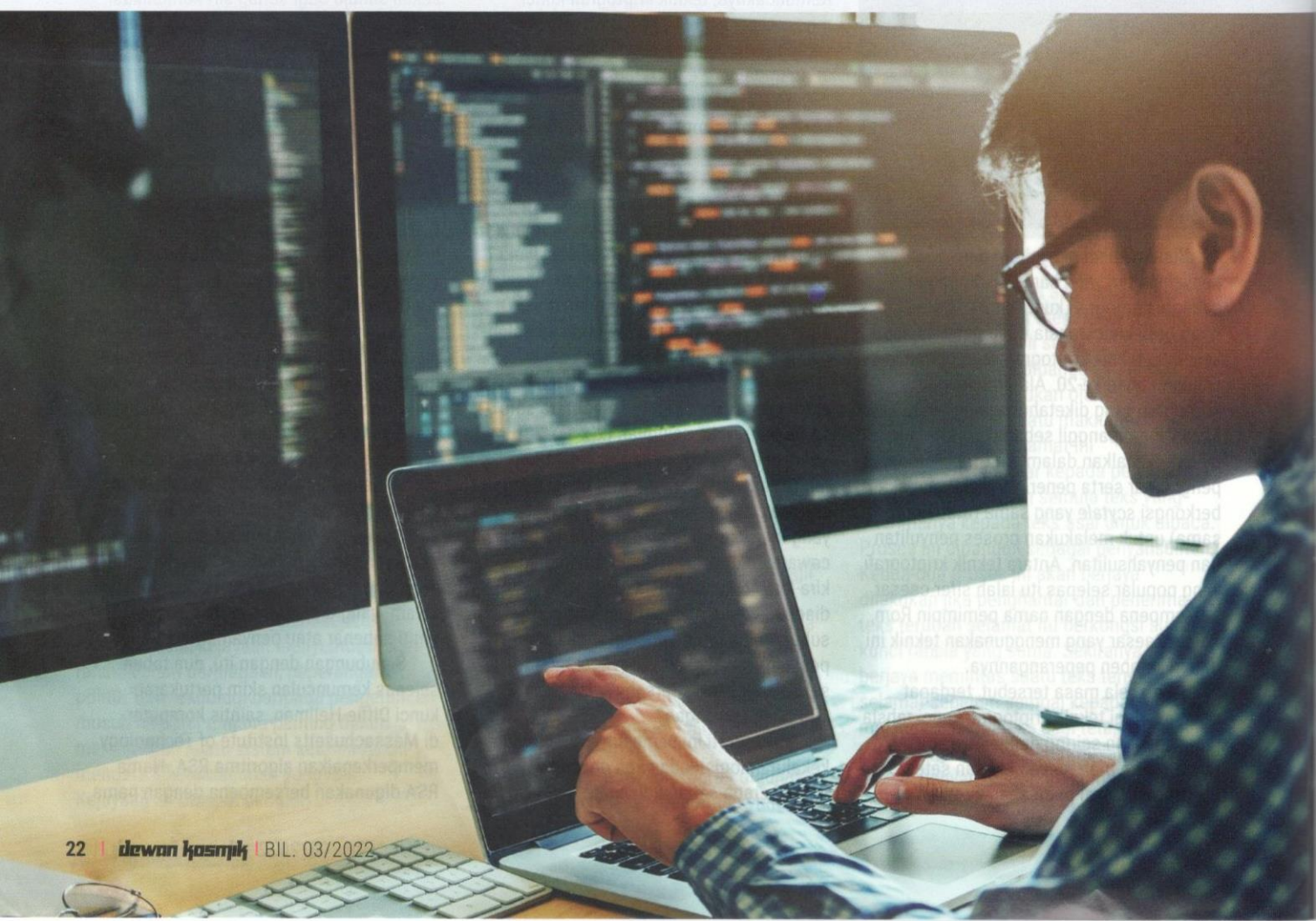
Dengan mengupayakan teorem matematik yang diperkenalkan oleh Leonhard Euler, RSA juga menggunakan masalah pemfaktoran integer, iaitu masalah teori nombor terkenal sebagai kekuatan gerak kerja algoritmanya. Secara teorinya, masa yang diperlukan untuk mencari kunci rahsia algoritma RSA (dan skim Diffie-Hellman) dengan proses cuba jaya akan memakan masa yang lebih lama berbanding dengan usia bumi sejak Letupan Besar berlaku.

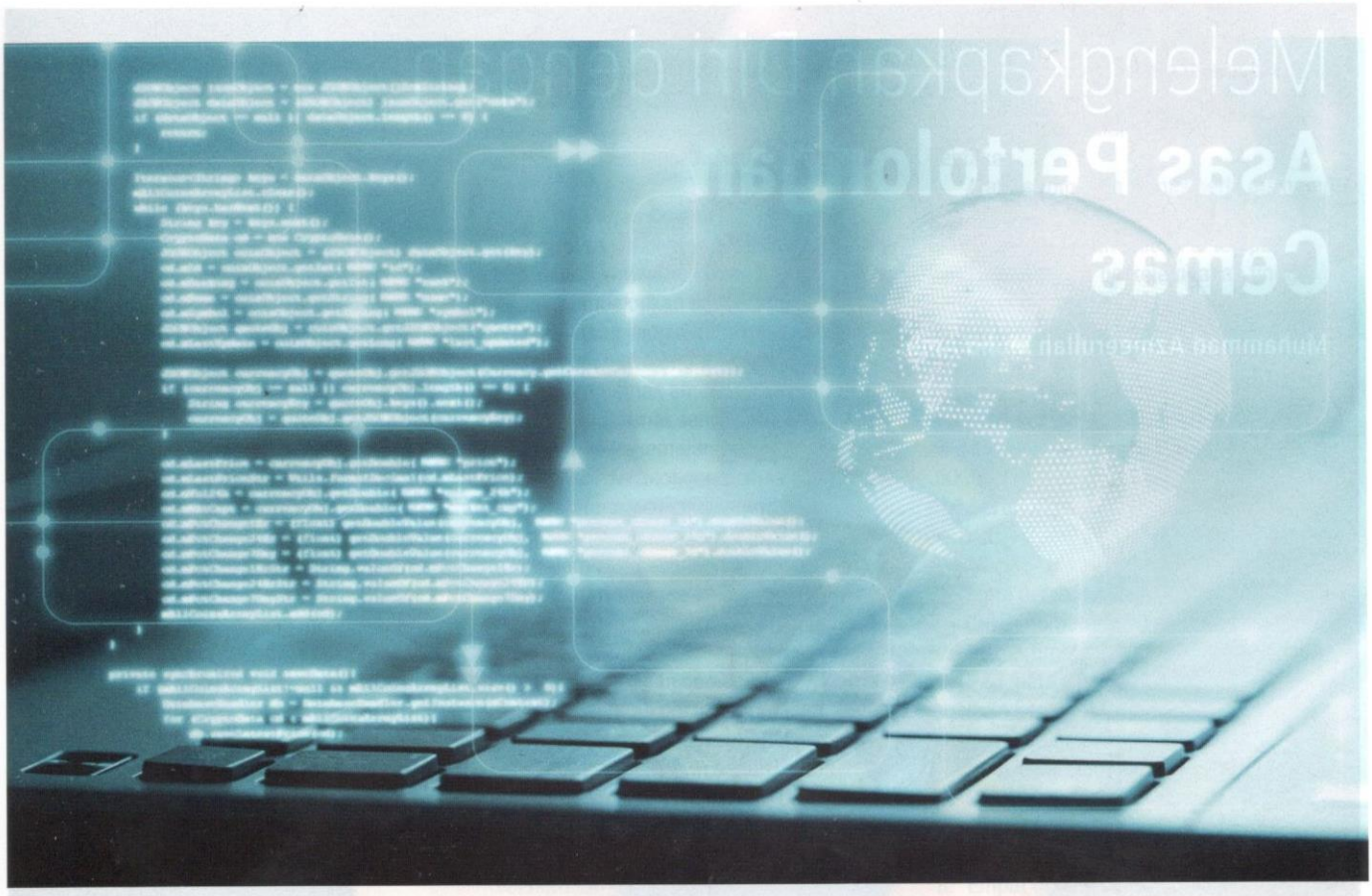
Kriptografi kunci awam menawarkan aplikasi matematik yang tampak terkedepan berbanding dengan teknologi komunikasi pada dekad 80-an. Walaupun mekanisme persetujuan kunci oleh skim Diffie-Hellman mampu menyelesaikan masalah pengagihan kunci, namun begitu penyelesaian ini hanya menjurus kepada operasi badan tertentu.

Di Malaysia, kesedaran untuk menggunakan elemen kriptografi dalam aplikasi digital dapat dilihat melalui pewartaan Akta Tandatangan Digital 1997 yang menyediakan rangka kerja perundangan ketika menggunakan sijil digital.

Pada waktu yang sama, fungsi penyulitan maklumat dan pengesahan identiti penghantar maklumat menggunakan algoritma RSA juga lebih banyak dibincangkan dalam dunia akademia berbanding dengan aplikasinya dalam kehidupan. Antara faktor yang menyebabkan keadaan ini berlaku ialah ketiadaan aplikasi harian yang sesuai. Selain itu, teknologi perhitungan digital juga masih berada pada peringkat primitif untuk mengaplikasikan perhitungan bermatematik yang digunakan oleh kriptografi kunci awam.

Walau bagaimanapun, segala-galanya berubah apabila era Internet bermula pada awal dekad 90-an. Peningkatan bilangan komputer peribadi, penambahan bilangan laman sesawang dan penggunaan mel elektronik yang menggunakan rangkaian telekomunikasi menyebabkan perlunya





pengguna Internet untuk menjamin keselamatan data digital dan kerahsiaan komunikasi sepanjang berada dalam talian. Hal ini diburukkan lagi dengan kemunculan serangan siber yang semakin meningkat.

Seperti orang mengantuk disorongkan bantal, mekanisme pertukaran kunci, penyulitan dan pengesahan identiti menggunakan kriptografi kunci awam hadir menyelamatkan komunikasi dunia digital dalam skala komersial. Bahkan, keupayaan komputer peribadi yang sudah mampu menghitung pengiraan nombor besar yang digunakan dalam kriptografi kunci awam, memacu adaptasi skim dan algoritma kriptografi kunci awam ke dalam perkakasan digital.

Kini, hampir setiap peranti dan aplikasi komunikasi digital yang digunakan mempunyai elemen kriptografi di dalamnya. Hal ini termasuklah gajet pintar dan peranti terbenam yang melengkapkan ekosistem digital yang dapat dilihat pada hari ini.

Di Malaysia, kesedaran untuk menggunakan elemen kriptografi dalam aplikasi digital dapat dilihat melalui pewartaan Akta Tandatangan Digital 1997 yang menyediakan rangka kerja perundangan ketika menggunakan sijil digital. Akta tersebut menekankan setiap sijil digital perlulah dikeluarkan oleh Pihak Berkuasa Pensijilan yang berlesen.

Dasar Kriptografi Negara yang telah diluluskan oleh kabinet pada tahun 2013 juga diharapkan mampu menyelaraskan kepatuhan jabatan, organisasi dan agensi kerajaan untuk melakukan penyulitan bagi melindungi data dan privasi. Dengan melaksanakan dasar ini secara menyeluruh, insiden kecurian data yang sering kali meresahkan pengguna aplikasi digital dapat dikurangkan kerana data yang dicuri itu akan berada dalam bentuk yang tidak boleh dibaca kerana telah disulitkan terlebih dahulu sebelum disimpan dalam pangkalan data.

Dalam Rancangan Malaysia Kesebelas (RMKe-11) yang telah tamat pada tahun 2020, CyberSecurity Malaysia dan para akademia dari universiti tempatan berjaya menggerakkan usaha menyenaraikan algoritma kriptografi terpercaya yang boleh digunakan oleh mana-mana pihak di Malaysia melalui projek Senarai Algoritma Kriptografi Terpercaya atau MySEAL. Melalui projek ini, semua agensi kerajaan dan syarikat komersial tempatan boleh merujuk senarai algoritma kriptografi yang selamat digunakan.

Kini, Pelan Strategi Keselamatan Siber Malaysia 2020-2024 diharapkan mampu menyuburkan penggunaan kriptografi yang terancang dalam setiap aplikasi digital kerajaan Malaysia. Hal ini dirancakkan lagi dengan ura-ura pengenalan inisiatif Identiti Digital Nasional di Malaysia.

Inisiatif ini diharapkan dapat mengintegrasikan elemen kriptografi kunci awam dan kriptografi kunci rahsia dalam pelaksanaannya sejajar dengan tujuan kriptografi, iaitu sebagai tunjang kemajuan komunikasi yang dipercayai dan boleh digunakan oleh suatu ketamadunan manusia.