KRIPTOGRAFI TEMPATAN DAN CABARANNYA

Disediakan oleh:

Prof. Madya Dr. Muhammad Rezal bin Dato' Kamel Ariffin

Pengarah, Institut Penyelidikan Matematik (INSPEM), Universiti Putra Malaysia
Penyelidik Kanan, Laboratori Kriptografi, Analisis dan Struktur, INSPEM, UPM

Emel: rezal@upm.edu.my

KANDUNGAN

1. RINGKASAN EKSEKUTIF

Kepentingan storan data serta berkomunikasi secara selamat melalui rangkaian terbuka adalah satu kemestian bagi institusi dan organisasi yang menghargai nilai keselamatan yang sedang dihantar. Storan data merujuk kepada penyimpanan data dalam suatu pangkalan data, Manakala komunikasi dalam rangkaian terbuka menggunakan infrastruktur awam seperti internet. Pemahaman tentang "**hacked**" data dan "**cracked**" data perlu jelas. Data boleh di **hack**, tetapi jika ianya dalam keadaan tersulit (**encrypted**) ianya tidak boleh dibaca, melainkan jika di **crack**. Tanpa menolak kepentingan infrastruktur keselamatan maklumat yang bersifat parameter luaran – pengurus keselamatan maklumat perlu mengimplementasi infrastruktur keselamatan maklumat **pertahanan terakhir – kriptografi.** Bagi kedua-dua jenis perkara, pengguna mempunyai pilihan sama ada menggunapakai aplikasi sedia ada (komersial) ataupun aplikasi yang dibangunkan sendiri. Yakni, pengguna mempunyai pilihan menggunakan kriptografi gred komersial atau lebih tinggi. Agensi-agensi keselamatan di negara maju seperti di Amerika Syarikat, National Security Agency (NSA) dan Central Security Service (CSS) memberi takrif berlainan serta menyediakan prasarana yang bebas dan berbeza dari entiti komersial untuk penyelesaian keselamatan maklumat infrastruktur kritikal.

Implementasi kriptografi secara betul dan selamat perlu menjadi agenda utama untuk mencapai gred keselamatan tertinggi. Pertimbangan implementasi kriptografi pada peringkat kerajaan perlu bebas dari reka bentuk keselamatan yang dibangunkan untuk kegunaan komersial. Implementasi juga perlu dibangunkan melalui metodologi yang betul serta dalam keadaan yang saintifik. Ini bermula dari peringkat asas yang melibatkan sains bermatematik, implementasi kriptografi dalam perisian atau perkakasan sehingga kepada amalan pengurusan kriptografi itu sendiri (i.e. *Public Key Infrastructure* (PKI)). Perkara ini perlu dilaksanakan secara terperinci dengan tujuan membangunkan Prasarana Kunci Awam Kerajaan (*Government Public Key Infrastructure* (GPKI)) yang mempunyai keselamatan bergred tinggi. Sepintas lalu, PKI ialah gabungan perkakasan, perisian, individu, polisi dan prosedur yang bertanggungjawab mewujudkan, mengurus, mengagihkan, mengguna, menyimpan dan membatalkan sijil digital serta menguruskan penyulitan kunci awam. Manakala, GPKI pula ialah Prasarana Kunci Awam Kerajaan yang digunakan oleh agensi sektor awam kerajaan Malaysia bagi memantapkan tahap keselamatan data dan maklumat sistem ICT kerajaan. GPKI di Malaysia telah diperkenalkan sejak tahun 2002 dalam pelaksanaan projek-projek Kerajaan Elektronik dan diuruskan oleh Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri.

2. TUJUAN DOKUMEN

Dokumen ini bertujuan untuk memberi input holistik kepada pembuat dasar yang bertanggungjawab kepada keseluruhan atau sebahagian dari implementasi penggunaan kriptografi di Malaysia. Justeru itu, dokumen ini antara lain mempunyai tujuan untuk memberi pencerahan kepada pembacanya dari sudut yang berikut:

I) Pemahaman elemen kriptografi yang utama iaitu penyulitan dan tandatangan digital;

II) Perundangan, dasar dan inisiatif sedia ada di Malaysia yang berkait dengan elemen kriptografi;

III) Isu kriptografi pasca kuantum (PQC), iaitu sistem kriptografi yang kebal serangan komputer kuantum;

IV) Perundangan, peraturan dan inisiatif antarabangsa yang berkait dengan pembekalan peralatan kriptografi yang bergred tinggi;

V) Memperkenalkan secara sepintas lalu beberapa agensi luar negara yang ditubuh khas untuk memacu isu kriptografi di negara masing-masing;

VI) Mengetengahkan isu-isu keselamatan berkaitan kriptografi.

Kandungan dokumen ini secara tersiratnya bertujuan untuk:

I) Memberi input aras tinggi kepada pembuat keputusan di Malaysia berkaitan kriptografi;

II) Memotivasikan pembuat keputusan untuk menubuhkan agensi khas untuk memacu isu kriptografi di Malaysia;

III) Memberi motivasi kepada pembuat keputusan untuk menyegerakan tindakan untuk memastikan kedaulatan negara terpelihara melalui penggunaan kriptografi yang bergred tinggi.

3. KRIPTOGRAFI SEPINTAS LALU

Pelaksanaan PKI berkesan didasari oleh pemahaman prinsip–prinsip asas kriptografi.

(a) Prinsip pertama: Permasalahan kriptografi yang diguna pakai dalam PKI perlu berasaskan takrif tepat dan padat keselamatan;

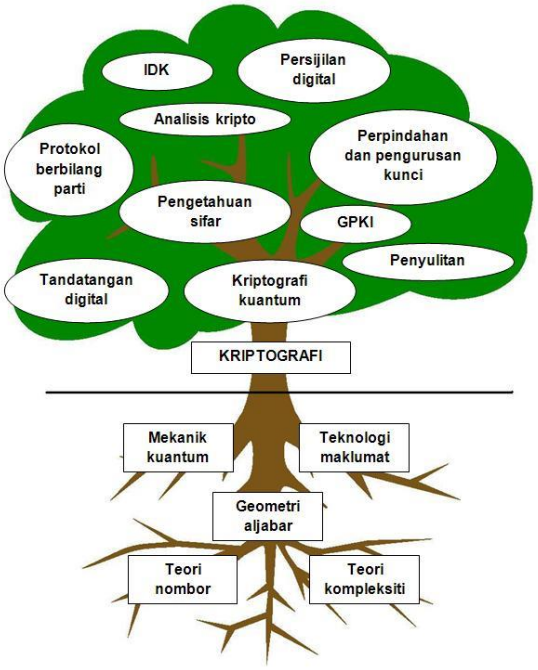
(b) Prinsip kedua: Apabila keselamatan pembangunan kriptografi dan kaedah pembekalan aplikasi kriptografi itu bergantung kepada andaian yang tidak terbukti, andaian ini mesti dinyatakan dengan jelas. Adalah lebih baik jika penggunaan andaian ini adalah pada tahap minimum; dan

(c) Prinsip ketiga: Penggunaan aplikasi kriptografi pada PKI yang dilaksanakan perlu diterangkan pembuktian keselamatannya bersandarkan kepada takrif yang dinyatakan dalam (a) dan juga secara relatif kepada andaian dalam (b).

Dalam memilih sistemkripto untuk diguna pakai, berikut merupakan panduan yang akan membantu:

(a) Kos untuk memecahkan algoritma **lebih tinggi** daripada nilai data (SELAMAT);
(b) Masa untuk memecahkan algoritma **lebih lama** daripada masa data perlu kekal berada dalam keadaan selamat (SELAMAT); dan
(c) Penggunaan sumber untuk menyulitkan data dengan sesuatu kunci **lebih rendah** daripada penggunaan sumber untuk memecahkan algoritma (SELAMAT).

Rajah di bawah memberi gambaran keseluruhan hubung kait antara ilmu yang mendasari kriptografi serta kedudukan aplikasi yang memerlukan kepada akar yang kuat kepada ilmu–ilmu tersebut bagi menjamin implementasi yang berkesan. Dari rajah di bawah, item GPKI, penyulitan, tandatangan digital dan IDK diperbincangkan secara khusus dalam seksyen berikutnya. Manakala perkara-perkara lain dalam rajah ini merupakan contoh-contoh lain yang mengguna pakai elemen kriptografi. Terdapat pelbagai lagi contoh yang tidak diilustrasikan di sini seperti kriptografi berasaskan identiti, fungsi cincang, nombor rawak sebenar dan lain-lain.



Rajah 1: Asas kepada kriptografi dan aplikasinya

4. TAKRIFAN

Takrifan yang perlu diambil maklum adalah seperti berikut:

(I) **Prasarana Kunci Awam (*Public Key Infrastructure* (PKI))** ialah satu set perkakasan, perisian, individu, teknologi, polisi, dan tatacara yang perlu bagi mencipta, mengurus, mengedar, mengguna, menyimpan dan membatalkan pemerakuan digital;

(II) **Penyulitan (*Encryption*)** ialah proses kriptografi yang menyulitkan teks asal kepada teks sulit untuk menghalangnya daripada diketahui oleh pihak yang tidak diingini;

(III) **Penyahsulitan (*Decryption*)** ialah proses kriptografi yang menyahsulitkan kembali teks sulit kepada teks asalnya;

(IV) **Tandatangan digital (Digital Signature)** ialah proses kriptografi yang menandatangani suatu dokumen digital bagi tujuan pengesahan identiti, memastikan data integriti dan menghalang kebolehsangkalan;

(V) **Fungsi cincang (*hash function*)** merujuk kepada suatu fungsi bermatematik yang akan menukarkan sebarang data kepada data yang tetap saiznya;

(VI) **Pembuktian keselamatan** merujuk kepada tahap keselamatan suatu sistemkripto yang boleh dibuktikan;

(VII) **Agensi sektor awam** ialah agensi yang merangkumi Kementerian, Jabatan Persekutuan, Badan Berkanun Persekutuan, Kerajaan Negeri, Badan Berkanun Negeri dan Pihak Berkuasa Tempatan;

(VIII) **Agensi pusat** ialah agensi sektor awam yang bertanggungjawab untuk menyelaras dan memantau pelaksanaan GPKI secara keseluruhan serta memberikan khidmat nasihat bagi penggunaan teknologi PKI bagi sistem ICT kerajaan dan mentadbir Portal GPKI;

(IX) **Agensi pelaksana** ialah agensi sektor awam yang memiliki aplikasi dan bertanggungjawab mengurus, menyelaras dan mentadbir sistem aplikasi yang menggunakan perkhidmatan GPKI;

(X) **Pihak Berkuasa Pemerakuan Berlesen [Licensed Certification Authority (CA)]** ialah pihak yang bertanggungjawab mengeluarkan sijil digital yang sah berdasarkan DSA dan Peraturan-Peraturan Tandatangan Digital 1998;

(XI) **Penghubung Pihak Berkuasa Pemerakuan [Bridge CA (BCA)]** ialah proses atau sistem yang dilaksanakan bagi menyelaras penggunaan sijil digital yang dikeluarkan oleh CA yang berbeza;

(XII) **Sijil digital** ialah perakuan yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) yang diguna pakai oleh pengguna atau pelayan untuk melaksanakan proses berikut:

(i) Menandatangan data digital;

(ii) Mengesahkan tandatangan data digital;

(iii) Mengesahkan tanpa penafian identiti; dan

(iv) Penyulitan data digital.

(XIII) **Medium sijil digital** ialah perkakasan atau perisian yang digunakan untuk menyimpan sijil digital pengguna. Beberapa medium yang digunakan adalah seperti yang berikut:

(i) **Kad Pintar**, iaitu kad yang mengandungi cip kriptografi untuk menyimpan sijil digital bagi melaksanakan fungsi Prasarana Kunci Awam (PKI). Kad ini dihubungkan kepada komputer pengguna menggunakan pembaca kad pintar;

(ii) **Token**, iaitu sebuah perkakasan yang mengandungi cip kriptografi untuk menyimpan sijil digital bagi melaksanakan fungsi Prasarana Kunci Awam (PKI). Perkakasan ini berbentuk seperti pemacu mudah alih dan dihubungkan kepada komputer pengguna menggunakan port USB; dan

(iii) **Sijil Perisian (*software certificate (softcert)*)** yang terdiri daripada:

i. **Sijil digital muat turun (*download certificate*)**, iaitu fail yang mengandungi sijil digital, kunci peribadi (*private key*) bagi pengesahan identiti, penyulitan data dan tandatangan digital. Sijil digital yang dijana boleh dimuat turun ke medium storan perkakasan pengguna dan lokasi sijil digital tidak tertakluk pada satu-satu komputer; dan

ii. **Sijil digital perayauan (*roaming certificate*)**, iaitu fail yang mengandungi sijil digital, kunci peribadi (*private key*) bagi pengesahan identiti, penyulitan data dan tandatangan digital. Sijil digital disimpan dalam pelayan yang berpusat di lokasi CA.

(XIV) **Sistem ICT kerajaan** ialah sistem yang merangkumi perkakasan, perisian, aplikasi, data, pengguna dan rangkaian dalam kerajaan;

(XV) **Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (Dasar Perkhidmatan GPKI)** ialah dokumen yang dikeluarkan dalam bentuk Pekeliling Kemajuan Pentadbiran Bilangan 3 Tahun 2015 oleh Jabatan Perdana Menteri pada 23 Oktober 2015.

(XVI) **Identiti Digital Kerajaan (IDK)** ialah inisiatif bagi setiap warganegara Malaysia memperkenalkan identiti secara digital yang selamat untuk digunakan.

5. ELEMEN ASAS YANG MENDASARI IMPLEMENTASI KRIPTOGRAFI KERAJAAN YANG EFEKTIF

Bahagian ini membincangkan elemen asas yang perlu ditangani agar pertanggungjawaban keselamatan maklumat dilaksanakan secara holistik. Amalan pertanggungjawaban kepada pihak ketiga yang seperti dilaksanakan oleh entiti komersial tidak boleh dijadikan piawai perkhidmatan sesebuah agensi kerajaan.

5.1 PENYULITAN

Penyulitan terbahagi kepada dua kaedah iaitu:

(i) Penyulitan simetri (menggunakan kunci yang sama untuk penyulitan dan penyahsulitan); dan

(ii) Penyulitan asimetri (menggunakan kunci awam untuk penyulitan dan kunci peribadi untuk penyahsulitan).

Dalam konteks PKI ianya merujuk kepada kaedah yang kedua. Beberapa risiko yang perlu diamati dalam penyediaan strategi penyulitan:

(i) Kegagalan untuk menyedari bahawa konsep penyulitan bukan hanya merujuk kepada algoritma yang diguna pakai, tetapi juga termasuk protokol penggunaannya serta pembuktian keselamatan protokol tersebut;

(ii) Penemuan kaedah analisiskripto terkini yang menyebabkan kaedah penyulitan yang diguna pakai tidak lagi selamat;

(iii) Proses dan kaedah pengurusan kunci;

(iv) Kegagalan organisasi untuk membuktikan amalan terbaik dalam melaksana pengurusan kunci yang memenuhi kehendak audit;

(v) Masalah sumber manusia. Ini lebih ketara jika proses pengurusan kunci adalah secara manual, mempunyai sistem pendokumentasian yang lemah dan kakitangan yang tidak terlatih; dan

(vi) Sesetengah proses penyulitan mungkin menggunakan masa pengkomputasian yang tinggi. Ini mungkin menyebabkan transaksi data itu perlahan dan mengehadkan kemampuan sistem itu untuk ditambah baiki.

Penyediaan prasarana penyulitan bermula dengan sumber kunci awam tersebut. Pembekalan elemen penyulitan perlu didasari dengan pengetahuan terkini teknologi analisis kripto dan juga teknologi pengkomputeran. Kedua–dua elemen ini perlu sentiasa diawasi dan difahami

agar sistem penyulitan yang disediakan sentiasa di atas paras selamat. Agensi yang bertanggungjawab untuk menyediakan perkhidmatan penyulitan ini juga perlu mempunyai tenaga pakar/mahir dalam menasihati takat pertanggungjawaban dan liabiliti yang sepatutnya. Pertanggungjawaban bagi pembekal prasarana penyulitan adalah seperti berikut:

(i) Memaklumkan pengguna mengenai perundangan yang melindungi mereka;

(ii) Memaklumkan pengguna tempoh masa data dijamin kekal selamat;

(iii) Menasihati pengguna kaedah penyulitan yang sesuai; dan

(iv) Melakukan penilaian semasa untuk mengesan data yang disulitkan dengan algoritma yang dianggap tidak lagi selamat digunakan.

5.2 TANDATANGAN DIGITAL

Seperti juga dalam pembekalan elemen penyulitan, pembekalan elemen tandatangan digital perlu didasari dengan pengetahuan terkini teknologi analisis kripto dan juga teknologi pengkomputeran. Secara asasnya, tandatangan digital merupakan kaedah yang bertujuan untuk membekalkan integriti kepada maklumat, kesahihan pengirim maklumat dan menghalang kemampuan pengirim maklumat untuk menafikan tindakannya mengirim maklumat tersebut.

Beberapa risiko yang perlu diamati dalam penyediaan strategi tandatangan digital:

(i) Kegagalan untuk menyedari bahawa konsep tandatangan digital bukan hanya merujuk kepada algoritma yang diguna pakai, malahan konsep ini juga termasuk protokol penggunaannya serta pembuktian keselamatan protokol tersebut;

(ii) Penemuan kaedah analisiskripto terkini yang menyebabkan kaedah tandatangan digital yang diguna pakai tidak lagi selamat;

(iii) Jika penyerang mampu menghasilkan tandatangan digital palsu dan menyalah guna tandatangan digital yang benar, ia akan menyebabkan sistem dan keseluruhan organisasi tidak dipercayai;

(iv) Jika pengurusan gagal menyediakan dokumentasi dan persijilan berkenaan polisi dan amalan berkaitan tandatangan digital serta pengurusan kunci, maka ia boleh menyebabkan suatu tandatangan digital itu tidak diterima pakai dalam suatu ruang lingkup pengurusan dan akhirnya tidak mempunyai nilai dalam organisasi tersebut; dan

(v) Sesetengah proses tandatangan digital mungkin menggunakan masa pengkomputasian yang tinggi. Ini mungkin menyebabkan transaksi data itu perlahan dan mengehadkan kemampuan sistem itu untuk ditambah baik.

5.3 AMALAN INFRASTRUKTUR/PRASARANA PENYULITAN DAN TANDATANGAN DIGITAL TERBAIK

Amalan prasarana terbaik dalam penyediaan tandatangan digital perlu melibatkan penjanaan:

(i) Sumber nombor rawak sebenar;

(ii) Kunci bayangan skim ambang (*Shadow Keys of the Threshold Scheme*);

(iii) Kunci awam dan persendirian skim penyulitan dan tandatangan digital tersebut;

(iv) Penggunaan fungsi cincang (*hash function*) yang terkini

(v) Penilaian kunci lemah

(vi) Pembuktian keselamatan penggunaan skim penyulitan dan tandatangan digital tersebut

(vii) Berdaftar sebagai pemilik kunci akar (*root key*);

(viii) Pengumpulan tinjauan bacaan berkenaan serangan terkini terhadap algoritma sedang diguna pakai; dan

(ix) Pembentukan kaedah penilaian penentuan sama ada algoritma yang diguna pakai masih utuh.

Setelah penjanaan kunci penyulitan dan tandatangan digital dijamin terpercaya, berikutnya adalah amalan pengurusan GPKI. Amalan pengurusan GPKI adalah seperti yang digariskan melalui Lampiran B dalam dokumen Dasar Perkhidmatan GPKI. Dalam lampiran tersebut, model pengurusan dan operasi perkhidmatan GPKI ditunjukkan melalui Rajah 1 . Ianya merangkumkan setiap pihak yang terlibat dalam pengurusan GPKI. Tanggungjawab setiap pihak ini juga ditunjukkan dalam Jadual 1 di lampiran yang sama.

6. PERUNDANGAN SERTA DASAR BERKAITAN YANG MEMANDU GERAK KERJA KRIPTOGRAFI DI MALAYSIA

Inisiatif gerak kerja kriptografi di Malaysia bukan terpisah dari perundangan serta dasar yang sedia ada. Ia merupakan satu lagi inisiatif yang berterusan untuk merealisasikan aspirasi kerajaan menuju negara yang maju menjelang 2020. Antara perundangan dan dasar berkaitan adalah seperti berikut:

6.1 AGENDA I.T NEGARA (NITA) – 1996

NITA memberi fokus kepada pembangunan sumber manusia, struktur–informasi dan aplikasi bagi menghasilkan nilai, memberi akses secara adil kepada rakyat Malaysia untuk mengubah secara kualitatif masyarakat Malaysia kepada masyarakat yang berasaskan pengetahuan menjelang tahun 2020. 5 agenda strategik kritikal yang akan memudah cara migrasi Malaysia ke *E-World* yang telah digariskan ialah:

(i) E-Masyarakat (*E-Community*);

(ii) E-Perkhidmatan Awam (*E-Public Services*);

(iii) E-Pembelajaran (*E-Learning*);

(iv) E-Ekonomi (*E-Economy*); dan

(v) E-Kedaulatan (*E-Sovereignty*).

6.2 AKTA TANDATANGAN DIGITAL (DSA) – 1997

Akta yang dimodelkan berasaskan Akta Tandatangan Digital Utah (1995) merupakan inisiatif kerajaan untuk menjadikan Malaysia suatu destinasi pelaburan pilihan syarikat-syarikat teknologi maklumat. Secara khususnya DSA menggariskan kaedah untuk dilantik menjadi Pihak Berkuasa Pemerakuan Berlesen [Certification Authority (CA)], tugas serta tanggungjawab CA dan keperluan pengguna tandatangan digital. Juga dimuatkan dalam perundangan ini ialah penerangan tentang isu-isu seperti pengiktirafan perundangan berkenaan tandatangan digital, liabiliti yang perlu ditanggung oleh CA dan penggunaan cop masa (*timestamp*). Walaupun perundangan ini memberi pengiktirafan kepada tandatangan digital bagi diumpamakan seperti tandatangan manual, terdapat satu elemen yang tidak dinyatakan iaitu keperluan rekod elektronik untuk dilayan sama seperti rekod salinan keras ataupun kontrak. Ini membawa maksud keperluan perundangan seperti keperluan menyimpan rekod mungkin tidak terpakai ke atas rekod elektronik. Juga perlu dinyatakan di sini jumlah liabiliti yang perlu ditanggung oleh CA jika tandatangan digital itu dipalsukan dan mengakibatkan kerugian pada penggunanya adalah tertakluk kepada Bab 8 DSA, iaitu suatu nilai kuantum (dalam Ringgit Malaysia) yang diperjelaskan terlebih dahulu oleh CA kepada pelanggannya. Justeru, GPKI perlu mengambil kira nilai maklumat kerajaan yang dipertanggungjawabkan ke atasnya dan memaklumkan kepada pihak CA untuk mendapat khidmat nasihat sewajarnya.

6.3 DASAR KESELAMATAN SIBER NEGARA (NCSP) – 2006

Dasar ini bertujuan untuk melaksanakan agenda melindungi agensi/organisasi CNII bagi merealisasikan visi ke arah persekitaran siber yang berdaya tahan dan berkemandirian. CNII Malaysia ditakrifkan sebagai aset (fizikal dan maya) sistem dan fungsi yang penting kepada negara kerana ketidakmampuan atau kehancurannya akan mempunyai impak dahsyat kepada:

(i) Kekuatan ekonomi negara;

(ii) Imej negara;

(iii) Keselamatan dan pertahanan negara;

(iv) Kemampuan kerajaan untuk berfungsi; dan

(v) Keselamatan dan kesihatan awam.

Seterusnya polisi ini telah mengenal pasti 10 sektor dalam Malaysia yang dikategorikan sebagai CNII. Iaitu:

(i) Keselamatan dan Pertahanan Negara;

(ii) Kewangan dan perbankan;

(iii) Komunikasi dan maklumat;

(iv) Tenaga;

(v) Pengangkutan;

(vi) Air;

(vii) Perkhidmatan kesihatan;

(viii) Kerajaan;

(ix) Perkhidmatan kecemasan; dan

(x) Makanan dan pertanian.

Polisi dibahagikan kepada 8 teras serta diamanahkan pemandu seperti Jadual 1.

Jadual 1: Teras Dasar Keselamatan Negara dan pemandunya

Bil.	Teras	Pemandu
1.	Tadbir urus berkesan	MKN
2.	Rangka kerja perundangan dan peraturan	PPN
3.	Rangka kerja teknologi keselamatan siber	KSTI
4.	Pembudayaan Keselamatan dan Pembangunan Sumber Manusia	KSTI

5.	R&D ke arah kemandirian	KSTI
6.	Pematuhan dan Penguatkuasaan	KKMM
7.	Kebersediaan menghadapi kecemasan keselamatan siber	MKN
8.	Kerjasama antarabangsa	KKMM

6.4 NATIONAL R&D ROADMAP FOR SELF RELIANCE IN CYBER SECURITY TECHNOLOGIES – 2011

Melalui inisiatif MIMOS, roadmap ini menyenaraikan bidang–bidang penyelidikan dan pembangunan yang diperlukan oleh Malaysia untuk kemandirian dalam teknologi keselamatan siber. Pelan ini telah dirumuskan oleh MIMOS dengan kerjasama suatu konsortium 22 buah organisasi yang mewakili akademia akademik, kerajaan, industri dan penyelidik yang bertujuan untuk mengintegrasikan dan mengurus semua program dan projek penyelidikan dan pembangunan (P&P) berkaitan keselamatan siber. Usaha ini bertujuan untuk mengelak duplikasi serta menggalakkan kerjasama antara akademik, industri dan kerajaan. Dengan dipandu oleh rangka kerja P&P yang bersepadu, hala tuju ini akan memberi fokus kepada teknologi yang akan melindungi Infrastruktur Maklumat Kritikal Negara [*Critical National Information Infrasturcture* (CNII) dengan matlamat untuk mencapai kemandirian dalam teknologi tersebut. Adalah diharapkan matlamat di atas akan tercapai dengan menambah usaha untuk mempromosikan penyelidikan keselamatan siber di institusi pengajian untuk menambah saiz komuniti penyelidik dalam bidang keselamatan siber ini. 7 bidang yang telah disenaraikan ialah:

(i) Komunikasi selamat (*Secure Communications*);
(ii) Sistem boleh diguna pakai tanpa hindaran;
(iii) Sistem sentiasa berada dalam keadaan kebersediaan (*High Availability Systems*);
(iv) Pengawasan, Tindakbalas dan Pemulihan (*Network Surveillance, Response and Recovery*);
(v) Hubungan terpercaya (*Trust Relationships*);
(vi) Akses selamat (*Secure Access*);
(vii) Kawalan Integriti Sistem (*System Integrity Controls*); dan
(viii) Jejak semula, Pengenalan dan Forensik (*Traceback, Identification and Forensics*).

6.5 DASAR KRIPTOGRAFI NEGARA (DKN) – 2013

Rangkaian telekomunikasi yang merentasi sempadan memungkinkan maklumat dipintas dan diakses secara tidak sah. Isu ketanpanamaan yang wujud di ruang siber kini pula menjadi halangan yang menyukarkan pengesahan identiti pengguna. Justeru, penggunaan kriptografi secara meluas dalam urusan elektronik peringkat Kerajaan kepada Kerajaan, Kerajaan kepada Rakyat, Kerajaan kepada Perniagaan dan Perniagaan kepada Perniagaan dilihat berupaya mewujudkan satu persekitaran siber yang selamat dan boleh dipercayai. DKN digubal bagi meningkatkan kecekapan dan mencapai kemandirian dalam penggunaan kriptografi ke arah kemakmuran ekonomi, kesejahteraan rakyat dan keselamatan negara. Ia juga menekankan kepentingan negara untuk menggunakan produk kriptografi terpercaya (yang telah melalui proses penilaian dan persijilan oleh agensi kerajaan yang dilantik) dalam semua aspek keselamatan maklumat. Malahan, dasar ini juga selari dengan NCSP dan dalam masa yang sama melengkapi NCSP. Pada ketika ini DKN berada di bawah seliaan *National Cyber Security Agency* (NACSA), Majlis Keselamatan Negara. Untuk mendukung dasar ini, 7 pelan strategik (PS) disediakan seperti dalam Jadual 2.

Jadual 2: Pelan Strategik DKN

Bil.	Pelan Strategik
1.	Pengwujudan mekanisme tadbir urus
2.	Pemantapan aspek perundangan dan peraturan
3.	Pemantapan pengurusan teknologi kriptografi
4.	Pembangunan dan pelaksanaan sistem penilaian dan persijilan produk kriptografi terpercaya
5.	Pembangunan keupayaan industri kriptografi tempatan
6.	Pembudayaan penggunaan kriptografi
7.	Penyelidikan dan pembangunan kriptografi

7. KRIPTOGRAFI PASCA KOMPUTER KUANTUM

Selari dengan perkembangan terkini teknologi pengkomputeran, suatu dokumen berkaitan amalan kritografi perlu juga bersifat terkehadapan dalam konteks mendepani cabaran keselamatan maklumat masa hadapan yang terdekat. Teknologi pengkomputeran berasaskan prosesor kuantum semakin menjadi realiti, ditambah pula dengan pendedahan terkini bahawa terdapat syarikat carian internet yang telah mempunyai teknologi tersebut.

7.1 TEKNOLOGI KUANTUM

Sekali imbas, berbeza dengan teknologi prosesor tradisional yang hanya boleh berada dalam keadaan “0”atau “1” pada satu–satu masa, prosesor kuantum boleh berada dalam keadaan “0” dan “1” pada satu–satu masa. Ini memberikan anjakan secara eksponen pada kemampuan prosesor tersebut. Perlu dimaklumkan di sini dari segi istilah “kriptografi pasca komputer kuantum” dan “kriptografi kuantum” adalah dua perkara berbeza. Kriptografi kuantum merujuk kepada metodologi menggunakan komputer kuantum untuk keselamatan maklumat. Manakala kriptografi pasca komputer kuantum merujuk kepada algoritma kriptografi (kebiasaannya merujuk kepada algoritma kunci awam) yang dibangunkan khusus untuk mengatasi kemampuan komputer kuantum tersebut. Pembangunan algoritma adalah berasaskan teori matematik yang dibuktikan secara matematik akan kemampuannya mengatasi serangan dari komputer kuantum. Pada masa kini, algoritma kunci awam yang popular adalah berasaskan kepada 3 permasalahan matematik iaitu: masalah pemfaktoran integer (contoh: RSA), masalah logaritma diskrit (contoh: pertukaran kunci Diffie Hellman) dan masalah logaritma diskrit lengkungan eliptik (contoh: ECC). Kesemua algoritma kunci awam yang didasari oleh elemen matematik yang disebut di atas, boleh diselesaikan dalam masa polinomial (i.e. diselesaikan dengan mudah) oleh algoritma Shor yang dijalankan atas komputer kuantum. Hasilnya, kunci rahsia boleh diperolehi. Maka, jika objektif asal ialah untuk melakukan penyulitan, ianya tidak akan tercapai kerana kunci rahsia boleh diperolehi dari kunci awam dan jika objektif ialah untuk melakukan tandatangan digital yang tidak boleh dipalsukan, ianya tidak akan tercapai kerana kunci tandatangan digital boleh diperolehi dari kunci pengesahan.

7.2 SISTEMKRIPTO PASCA KUANTUM

Terkini, antara elemen matematik yang telah diguna pakai untuk menghasilkan sistemkripto pasca komputer kuantum ialah:

(i) Sistemkripto berasaskan kekisi (contoh: NTRU oleh Security Innovation Inc);
(ii) Sistemkripto multivariat (contoh: SFLASH oleh NESSIE);
(iii) Sistemkripto berasaskan cincangan (contoh: Skim tandatangan Merkle); dan
(iv) Sistemkripto berasaskan kod (contoh: sistemkripto McEliece).

Di peringkat antarabangsa, kerja–kerja untuk menghadapi cabaran pasca komputer kuantum telah mendapat perhatian yang semakin serius oleh ahli akademia dan industri. Suatu siri persidangan antarabangsa yang khusus membincangkan isu–isu berkaitan hal ini telah dimulakan sejak 2006, iaitu persidangan PQCrypto. Di Eropah telah diadakan *European Telecommunications Standards Institute (ETSI) Workshops on Quantum Safe Cryptography*. Pada Jun 2015, ETSI telah mengeluarkan kertas putih bertajuk "*Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges*". Di Amerika Syarikat, Agensi Keselamatan Kebangsaannya (NSA) telah mengeluarkan pekeliling kepada jabatan–jabatan kerajaannya untuk bersedia berpindah kepada algoritma pasca komputer kuantum pada Ogos 2015. Manakala jabatan piawaian Amerika Syarikat iaitu *National Institute of Standards and Technology* (NIST) telah mengeluarkan laporan *Report on Post-Quantum Cryptography* pada Februari 2016. Di United Kingdom, organisasi *Government Communications Headquarters* (GCHQ) telah memulakan inisiatif untuk bekerjasama dengan akademia dan industri untuk menghadapi cabaran baru ini.

7.3 TATACARA PENYEDIAAN DAN IMPLEMENTASI PRASARANA KRIPTOGRAFI PASCA KOMPUTER KUANTUM TERBAIK

Bagi menyediakan prasarana kriptografi pasca kuantum, berikut adalah tatacara terbaik:

(i) Penyediaan jabatan dengan kakitangan yang kompeten isu–isu terkini pengkomputeran kuantum;
(ii) Penyediaan jabatan dengan kakitangan yang kompeten untuk mendepani isu–isu teknikal PKI pasca kuantum;
(iii) Menyediakan sekurang–kurang 2 set PKI pasca kuantum untuk kegunaan objektif penyulitan dan tandatangan digital. Perlu lebih dari 2 untuk tahap jaminan yang berlainan;
(iv) Penyediaan perkakasan selamat untuk menjana kunci asimetri pasca kuantum;
(v) Penyediaan API untuk berinteraksi dengan pelayar dan pelayan; dan
(vi) Penyediaan suatu sistem penjanaan kunci yang boleh mengenal pasti kunci lemah.

8. WASENNAR ARRANGEMENT

Peraturan yang dikenali sebagai *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* yang telah mula disepakati pada July 1996, adalah suatu rejim kawalan eksport multilateral yang dianggotai oleh 42 buah negara. Negara yang terlibat ialah Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom dan Amerika Syarikat. Antara tujuan peraturan ini ialah supaya dapat memastikan kestabilan dan keselamatan serantau dengan mempromosikan transperensi dan pertanggungjawaban dalam pengagihan peralatan senjata konvensional serta barangan yang mempunyai dwi-kegunaan, agar boleh menghalang longgokkan persenjataan yang boleh menyahstabilkan keadaan. Setiap negara yang terlibat dalam peraturan ini perlu memastikan bahawa polisi negara masing-masing akan menentukan pengagihan peralatan yang disenaraikan tidak akan memangkinkan pembangunan dan penambahbaikan keupayaan ketenteraan yang boleh menyebabkan objektif peraturan ini tidak akan tercapai. Senarai asas mengandungi 10 kategori peralatan. Iaitu:

- Kategori 1 – *Special Materials and Related Equipment*
- Kategori 2 – *Materials Processing*
- Kategori 3 – *Electronics*
- Kategori 4 – *Computers*
- Kategori 5 – *Part 1 – Telecommunications*
- Kategori 5 – *Part 2 – Information Security*
- Kategori 6 – *Sensors and Lasers*
- Kategori 7 – *Navigation and Avionics*
- Kategori 8 – *Marine*
- Kategori 9 – *Aerospace and Propulsion*

Wassenaar Arrangement

on

Export Controls for Conventional Arms and
Dual-Use Goods and Technologies

PUBLIC DOCUMENTS

Volume II

List of Dual-Use Goods and Technologies
and
Munitions List

Compiled by the Wassenaar Arrangement Secretariat
December 2019

Rajah 1: Dokumen Umum Peraturan Wasennar Jilid II (Disember 2019)

Rujuk mukasurat 93 – 100 Peraturan Wasennar Jilid II (Disember 2019). Antara lain:

- Fungsi kriptografi tidak boleh ditukar oleh pengguna (ms 93);
- Keperluan minima kunci kriptografi yang sangat tidak selamat (ms 95);
- Bahagian kemampuan kriptografi tidak boleh diubahsuai oleh pengguna (ms 96);
- Penyediaan kemampuan yang boleh mengatasi sistemkripto (ms 99)

Justeru, syak bahawa peralatan kriptografi yang dibekal dari negara-negara yang mempersetujui Peraturan Wasennar tidak selamat, bukanlah suatu syak yang tidak berasas. Pihak kerajaan perlu ambil maklum akan hal ini dan mendalami lagi kandungan Peraturan Wasennar tersebut.

9. INTERNATIONAL TRAFFIC IN ARMS REGULATIONS

International Traffic in Arms Regulations (ITAR) merupakan perundangan Amerika Syarikat yang mengawal dan menghadkan eksport teknologi berkaitan ketenteraan dan pertahanan untuk tujuan menjaga keselamatan dan menjayakan polisi luar negara Amerika Syarikat. Antara tahun 1996 – 1997, kriptografi disenaraikan dalam senarai U.S Munitions List dan

dihalang eksport ke luar Amerika Syarikat. Walaupun tidak lagi disenaraikan dalam U.S Munitions List, namun syak bahawa eksport peralatan kriptografi dari Amerika Syarikat bukan merupakan peralatan gred tinggi, masih ada.

10. GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR merupakan peraturan undang-undang EU mengenai perlindungan dan privasi data di Kesatuan Eropah (EU) dan Kawasan Ekonomi Eropah (EEA). Ianya juga menangani pemindahan data peribadi di luar kawasan EU dan EEA. Tujuan utama GDPR ialah untuk memberikan kawalan kepada individu atas data peribadi mereka dan untuk mempermudahkan persekitaran pengawalseliaan untuk perniagaan antarabangsa dengan menyatukan peraturan dalam EU. GDPR juga mengandungi peruntukan dan keperluan yang berkaitan dengan pemprosesan data peribadi individu (secara formal dipanggil subjek data dalam GDPR) yang tinggal di EEA, dan terpakai kepada mana-mana perusahaan-tanpa mengira lokasi dan kewarganegaraan subjek data atau tempat tinggal yang memproses maklumat peribadi subjek data di dalam EEA. Justeru, Malaysia perlu menaiktaraf infrastruktur kriptografinya untuk memastikan pertahanan keselamatan terakhir data diperkuatkan. Ianya akan menjadi suatu situasi yang memalukan sekiranya data peribadi rakyat EU didapati bocor semasa dalam penjagaan agensi kerajaan Malaysia mahupun entiti swasta di Malaysia.

11. BADAN SELIAAN KRIPTOGRAFI NEGARA LAIN

Seksyen ini akan membincangkan beberapa agensi terpilih yang melaksanakan tanggungjawab mengurus kriptografi di negara masing-masing. Pelaporan dalam seksyen ini hanyalah ringkasan. Untuk maklumat lanjut, pembaca boleh ke laman web agensi tersebut.

11.1 NATIONAL SECURITY AGENCY (NSA), AMERIKA SYARIKAT

NSA yang telah ditubuhkan pada tahun 1952, merupakan badan yang menguruskan keperluan kriptografi di Amerika Syarikat. Di bawah seliaan NSA, terdapat 2 set algoritma kriptografi yang dikenali sebagai Suite A dan Suite B. Suite A merupakan algoritma kriptografi berklasifikasi tinggi manakala Suite B pula adalah untuk kegunaan umum. NSA memastikan Amerika Syarikat menggunakan sistemkripto gred tinggi untuk kedaulatannya.

11.2 GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ), UNITED KINGDOM

Pada asalnya GCHQ telah ditubuhkan selepas Perang Dunia Pertama sebagai Government Code and Cypher School (GC&CS). Semasa Perang Dunia Kedua, kakitangannya bertanggungjawab untuk memecahkan kod Jerman Nazi yang menggunakan peralatan bernama Enigma. Terkini, GCHQ mempunyai 4 teras utama seperti berikut:

- *Sigint missions: comprising mathematics and cryptanalysis, IT and computer systems, linguistics and translation, and the intelligence analysis unit*
- *Enterprise: comprising applied research and emerging technologies, corporate knowledge and information systems, commercial supplier relationships, and biometrics*
- *Corporate management: enterprise resource planning, human resources, internal audit, and architecture*
- *Communications-Electronics Security Group*

11.3 BADAN SIBER DAN SANDI NEGARA (BSSN), INDONESIA

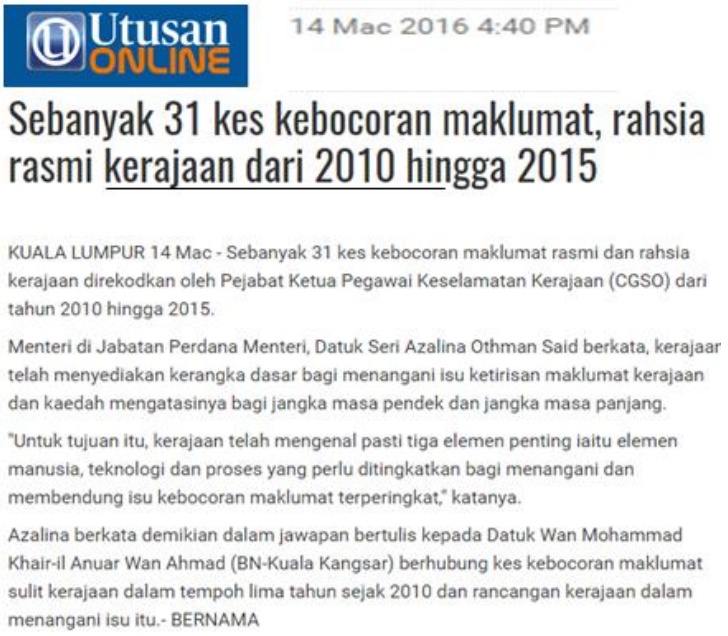
Badan yang menyelenggara elemen kriptografi (i.e.persandian) di Indonesia bermula sejak tahun 1946 dan dikenali sebagai Dinas Code. Jabatan ini mempunyai peranan yang amat penting dalam usaha mencapai kemerdekaan dan urusan pentadbiran selepas kemerdekaan. Jabatan ini dinaik taraf menjadi Lembaga Sandi Negara pada tahun 1972. Pada tahun 2003, Indonesia menubuhkan Sekolah Tinggi Sandi Negara untuk memenuhi keperluan sumber manusia dalam bidang kriptografi di Indonesia. Pada tahun 2017, Indonesia menubuhkan Badan Siber dan Sandi Negara yang bertanggungjawab terus kepada Presiden. BSSN bukan merupakan entiti baru. Ianya adalah suatu badan yang menaiktaraf lembaga sebelumnya iaitu Lembaga Sandi Negara dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika. Dengan terbentuknya BSSN, maka pelaksanaan seluruh tugas dan fungsi bidang persandian di Lembaga Sandi Negara serta pelaksanaan seluruh tugas dan fungsi di bidang keselamatan informasi, keselamatan jaringan telekomunikasi berasaskan protokol internet, dan keselamatan jaringan dan infrastruktur telekomunikasi yang berada di Kementerian Komunikasi dan Informatika dilaksanakan oleh BSSN.

12. KES TIADA PENGGUNAAN KRIPTOGRAFI

12.1 KEBOCORAN DATA RASMI NEGARA

Kebocoran data rasmi negara bukan merupakan perkara yang luar biasa. Ini kerana metodologi keselamatan maklumat tidak bersandarkan kepada implementasi kriptografi. Hanya dengan elemen penyulitan, sekiranya suatu data itu diperolehi dengan cara "**hacking**"- data itu perlu di "**crack**" yakni dinyahsulit sebelum oleh dibaca. Hakikatnya, tanpa elemen penyulitan, suatu data yang diperolehi secara "**hacking**" boleh terus dibaca oleh musuh.

Adalah menjadi suatu "jenayah" bagi agensi yang bertanggungjawab untuk memastikan data rasmi negara kekal rahsia tetapi gagal untuk menjalankan amanah dengan sebaiknya. Justeru, suatu pendekatan yang lebih strategik yang melibatkan penggunaan kriptografi sepenuhnya mesti diwujudkan. Berikut adalah petikan akhbar pada tahun 2016 yang berkaitan dengan kebocoran rahsia kerajaan. Andaiannya ialah data tersebut berada dalam bentuk elektronik. Terkini, tiada lagi laporan akhbar yang sensasi begini. Namun, tanpa elemen kriptografi keselamatan data belum terjamin sepenuhnya.



Utusan ONLINE

14 Mac 2016 4:40 PM

Sebanyak 31 kes kebocoran maklumat, rahsia rasmi kerajaan dari 2010 hingga 2015

KUALA LUMPUR 14 Mac - Sebanyak 31 kes kebocoran maklumat rasmi dan rahsia kerajaan direkodkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO) dari tahun 2010 hingga 2015.

Menteri di Jabatan Perdana Menteri, Datuk Seri Azalina Othman Said berkata, kerajaan telah menyediakan kerangka dasar bagi menangani isu ketirisan maklumat kerajaan dan kaedah mengatasinya bagi jangka masa pendek dan jangka masa panjang.

"Untuk tujuan itu, kerajaan telah mengenal pasti tiga elemen penting iaitu elemen manusia, teknologi dan proses yang perlu ditingkatkan bagi menangani dan membendung isu kebocoran maklumat terperingkat," katanya.

Azalina berkata demikian dalam jawapan bertulis kepada Datuk Wan Mohammad Khair-il Anuar Wan Ahmad (BN-Kuala Kangsar) berhubung kes kebocoran maklumat sulit kerajaan dalam tempoh lima tahun sejak 2010 dan rancangan kerajaan dalam menangani isu itu.- BERNAMA

Rajah 3: Keratan berita pada tahun 2015

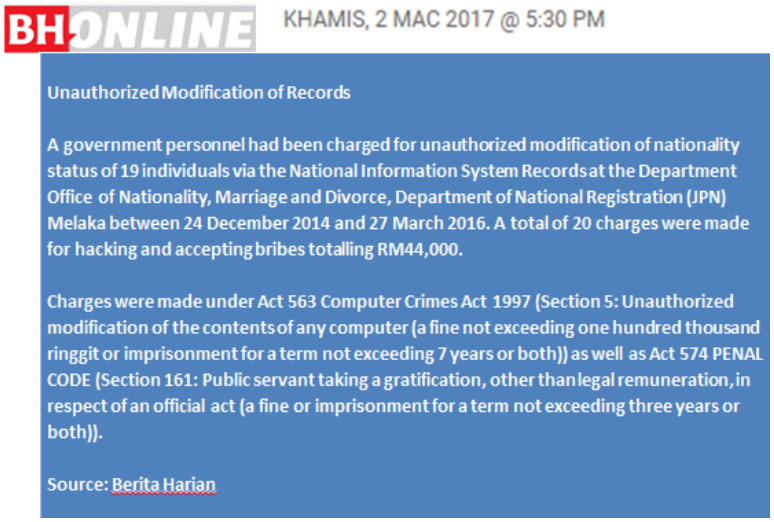
12.2 KEBOCORAN DAN PERUBAHAN GERAN HAK MILIK TANAH

Malaysia juga mencatat kes yang melibatkan perubahan maklumat pada geran hak milik tanah. Ini adalah disebabkan data tidak melalui proses penyulitan terlebih dahulu. Tambahan pula, sistem tidak mempunyai mekanisma tandatangan digital, yakni tidak ada proses pengesahan si penukar maklumat.

Rajah 4: Kes tukar kandungan geran tanah. Dokumen ini tidak boleh diakses lagi.

12.3 KEBOCORAN DAN PERUBAHAN STATUS KEWARGANEGARAAN

Kes perubahan status kewarganegaraan juga pernah berlaku di Malaysia. Tanpa elemen penyulitan jenayah ini tiada halangan terakhir – data yang disulitkan (**encrypted**).



Rajah 5: Kes ubah status kewarganegaraan

13. KES PENGGUNAAN KRIPTOGRAFI LEMAH

13.1 KAD IDK RAKYAT TAIWAN

Penggunaan kriptografi perlulah dianalisa dengan terperinci oleh agensi dalaman sesebuah negara. Kenyataan bahawa sesuatu aplikasi kriptografi itu selamat tidak boleh diterima bulat-bulat walaupun telah melepasi piawaian tertentu. Kelemahan yang telah melumpuhkan program Sijil Digital Citizen Taiwan menimbulkan keraguan terhadap pensijilan produk yang telah digunapakai. Kelemahan kriptografi Sijil Digital Citizen Taiwan telah dibentangkan dalam satu kertas di persidangan Asiacrypt 2013 di Bangalore, India. Kelemahan yang telah dikenalpasti ini berpunca dari peralatan yang turut digunapakai oleh banyak negara lain, walaupun peralatan ini lulus piawaian FIPS 140-2 Tahap 2 dan Common Citeria. Secara teorinya, persijilan peralatan ini yang dikendalikan oleh Institut Teknologi dan Teknologi Kebangsaan (NIST) dan rakan sejawatnya di seluruh dunia, telah pun melalui penilaian dengan syarat yang ketat ke atas perkakasan dan perisian kriptografi yang akan diguna oleh agensi kerajaan.

Raising troubling questions about the reliability of government-mandated cryptography certifications used around the world, scientists have unearthed flaws in Taiwan's secure digital ID system that allow attackers to impersonate some citizens who rely on it to pay taxes, register cars, and file immigration papers.

Rajah 6: Kes IDK Rakyat Taiwan 2013.

(https://arstechnica.com/information-technology/2013/09/fatal-crypto-flaw-in-some-government-certified-smartcards-makes-forgery-a-snap/)

13.2 KAD IDK RAKYAT ESTONIA

Pada tahun 2017, Estonia jug mengalami kes yang sama seperti Taiwan.

Rajah 7: Kes IDK Rakyat Estonia 2017.

(https://www.bbc.com/news/technology-41858583)

13.3 CRYPTO AG

Pada bulan Mac 2020 telah didedahkan bahawa CryptoAG, sebuah syarikat pembekalan peralatan kriptografi, telah membekalkan peralatan yang menggunakan elemen keselamatan maklumat yang tidak menjalankan fungsi seperti yang dinyatakan. Berpuluh negara menggunakan peralatan tersebut. Malaysia tidak terkecuali. Malaysia telah menggunakan peralatan CryptoAG sejak sekian lama. Ini merupakan suat perkara yang amat merbahaya serta memalukan.

Rajah 8(a): Berita Malaysia menggunakan peralatan CryptoAG yang membocorkan rahsia negara.

The logo of Crypto AG is seen at its headquarters in Steinhausen, Switzerland Feb 11,2020. - Reuters

WASHINGTON, United States (AFP): US and German intelligence services raked in the top secret communications of governments – including Malaysia's – around the world for decades through their hidden control of a top encryption company, Crypto AG, US, German and Swiss media reported Tuesday (Feb 11).

Rajah 8(b): Berita Malaysia menggunakan peralatan CryptoAG yang membocorkan rahsia negara.

14. LAPORAN THALES 2020

Thales merupakan sebuah syarikat multinasional Perancis yang merekabentuk dan membina sistem elektrikal serta memberi perkhidmatan untuk sektor aeroangkasa, pertahanan, pengangkutan dan bursa saham. Thales e-security merupakan cabang perkhidmatan dan perniagaan Thales yang berkait dengan keselamatan maklumat khususnya unsur kriptografi. Setiap tahun Thales mengeluarkan laporan mengenai keadaan semasa amalan keselamatan maklumat peringkat global. Berikut adalah intipati laporan tahun 2020.

Rajah 9: Laporan Thales 2020

Rajah 10: Penemuan utama dalam laporan Thales 2020

15. SENARAI ALGORITMA KRIPTOGRAFI TERPECAYA NEGARA (MySEAL)

Projek MySEAL adalah usaha yang bermula dari 2016-2020, yang akan digunakan sebagai keperluan dan garis panduan penggunaan algoritma kriptografi dalam semua produk kriptografi yang dipercayai di Malaysia.

MySEAL adalah sebuah projek untuk membangunkan satu portfolio algoritma kriptografi kebangsaan yang dipercayai. Ia merupakan projek yang direka khusus untuk menyediakan senarai algoritma kriptografi yang sesuai untuk pelaksanaan dalam konteks Malaysia yang menyokong Dasar Kriptografi Dasar (NCP). Dokumen NCP berfungsi sebagai dokumen panduan bagi Malaysia untuk mencapai kedaulatan kriptografi manakala MySEAL akan menyokong bidang saintifik kriptografi dan analisiskripto.

Disamping itu, MySEAL adalah untuk menggalakkan kerjasama strategik, penyelidikan dan pengeluaran sistem kriptografi oleh industri tempatan, yang membolehkan mereka mengemukakan algoritma kriptografi mereka untuk ujian dan pengesahan oleh pemeriksa sebelum algoritma boleh diakui sebagai algoritma kriptografi yang dipercayai di peringkat

kebangsaan. Untuk suatu algoritma kriptografi boleh disenaraikan dalam MySEAL, ia perlu mematuhi kriteria seperti yang dinyatakan dalam Projek MySEAL: Kriteria Penyerahan dan Penilaian Versi 1.0 [2016]. Kriteria ini telah dibangunkan berdasarkan piawaian dan syarat antarabangsa yang diterima oleh jawatankuasa Kumpulan Fokus MySEAL. Jawatankuasa ini diterajui oleh CyberSecurity Malaysia dan disokong oleh ahli-ahli dari institusi di Malaysia.

Semasa pusingan pertama projek MySEAL, ia hanya menerima fungsi hash simetri, asimetrik, kriptografi dan primitif penjanaan utama kriptografi. Algoritma untuk setiap primitif akan diperolehi dalam dua cara; panggilan untuk penyerahan algoritma baru, dan algoritma dari standard sedia ada termasuk dari projek penyenaraian algoritma kriptografi yang dipilih oleh jawatankuasa yang dilantik. Semua algoritma akan diperiksa dan kemudiannya dinilai secara menyeluruh berdasarkan kriteria penilaian dan akhirnya, algoritma yang dipilih akan diumumkan.

Inisiatif MySEAL bukanlah suatu usaha kecil. Sejak dokumentasi Agenda IT Nasional (NITA) pada tahun 1996 yang menyenaraikan e-Sovereignty sebagai salah satu objektif Malaysia memasuki era Teknologi Maklumat (IT), pelaksanaan MySEAL adalah salah satu tonggak utama bagi Malaysia. Melalui inisiatif ini, Malaysia akan memasuki bidang dasar keselamatan maklumat yang merupkan suatu arena yang mencabar. Ini akan membuktikan ketekunan dan stamina Malaysia dalam melindungi infrastruktur maklumatnya di peringkat algoritma kriptografi.

16. PERSATUAN PENYELIDIKAN KRIPTOLOGI MALAYSIA

Selepas kejayaan Persidangan Kriptologi Kebangsaan Pertama dan ke-2 pada tahun 2004 dan 2006 yang dianjurkan oleh Institut Penyelidikan Matematik, Universiti Putra Malaysia, cadangan telah dimajukan untuk pembentukan sebuah persatuan penyelidikan kriptologi oleh masyarakat kriptologi Malaysia. Jawatankuasa pro-tem mengemukakan permohonan itu kepada Pendaftar Pertubuhan Malaysia dan persatuan telah ditubuhkan pada tahun 2007.

Persatuan Penyelidikan Kriptologi Malaysia (MSCR) adalah organisasi bukan berteraskan keuntungan yang terdiri daripada ahli akademik, penyelidik, pakar, pelajar dan institusi yang berminat untuk melanjutkan penyelidikan dalam bidang kriptologi dan bidang yang berkaitan. MSCR juga secara berkala mempamerkan pandangannya sebagai masyarakat

penyelidikan utama dalam bidang kriptologi dalam merealisasikan potensi kriptografi penuh untuk Malaysia. Sejak penubuhannya, ia telah terlibat secara aktif bersama-sama pelbagai agensi yang mencari nasihat berkaitan dengan kriptografi dan kriptologi secara umum. Disamping itu, MSCR, mengalu-alukan ahli-ahli baru untuk memajukan idea-idea baru mengenai cara menjalankan aktiviti-aktiviti dalam bidang berkaitan kriptologi di Malaysia.

17. AKADEMIA DAN PENYELIDIKAN KRIPTOGRAFI DI MALAYSIA

Antara universiti yang mempelopori penyelidikan kriptologi secara aktif di Malaysia ialah Universiti Putra Malaysia, Universiti Teknikal Malaysia Melaka, Universiti Multimedia Malaysia dan Universiti Tunku Abdul Rahman. Terdapat juga aktivti kriptografi di Universiti Sains Malaysia, Universiti Teknologi MARA dan Universiti Tenaga Nasional. Di peringkat agensi kerajaan, penyelidikan didapati berlaku di CyberSecurity Malaysia (CSM) dan MIMOS.

Penyelidikan kriptografi bermatematik secara aktif, yakni penyelidikan pembangunan kriptografi dari asas fundamental hingga ke prototaip boleh didapati di Laboratori Kriptografi, Analisis dan Struktur, Institut Penyelidikan Matematik, UPM.

18. INDUSTRI KRIPTOGRAFI SEDIA ADA DI MALAYSIA

Untuk tidak berat sebelah, laporan ini hanya akan mengenalpasti kapasiti industri kriptografi di Malaysia secara umum.

18.1 KEPERLUAN AWAM – KERAJAAN

Terdapat syarikat di Malaysia yang berupaya untuk menyediakan elemen kriptografi yang diasimilasikan dengan platform kerajaan sedia ada.

18.2 KEPERLUAN AWAM – PERBANKAN

Terdapat syarikat di Malaysia yang berupaya untuk menyediakan elemen kriptografi yang diasimilasikan dengan platform perbankan sedia ada.

18.3 KEPERLUAN ANTARABANGSA

Terdapat syarikat hak milik rakyat Malaysia yang melakukan pembangunan dan penyelidikan kriptografi dan aplikasi perkakasannya. Syarikat ini telah memasarkan peralatan tersebut ke agensi strategik di Eropah dan Jepun.

19. JALAN KE HADAPAN

Berikut merupakan cadangan garis masa aras tinggi untuk menjayakan agenda penggunaan kriptografi bergred tinggi di Malaysia. Dianggarkan memakan masa 48 bulan.

Bulan	Perkara	Catatan
1-3	Mengadakan mesyuarat khas dengan semua agensi di Malaysia yang mengendalikan kriptografi dengan matlamat mewujudkan agensi khas yang memacu isu kriptografi di Malaysia.	Perlu kepada arahan dari pihak tertinggi di Malaysia iaitu Perdana Menteri. Sebagai catatan, Tan Sri Muhyiddin Yassin merupakan Timbalan Perdana Menteri pada tahun 2013 yang mempengerusikan Jawatankuasa E-Kedaulatan dan telah memperakukan Dasar Kriptografi Negara pada ketika itu sehingga ke tahap kelulusan Kabinet.
4-6	Menyiapkan kertas kerja menggerakkan agenda kriptografi yang mengandungi anggaran peruntukkan.	i) Untuk makluman, Infrastruktur Kunci Awam Kerajaan (GPKI) yang membekalkan elemen tandatangan digital sahaja kepada agensi kerajaan (bukan pegawai kerajaan secara individu – tetapi jabatan yang berkaitan) mempunyai kos anggaran sebanyak RM30juta-40juta untuk tempoh 2-3 tahun. Perkhidmatan GPKI perlu di tambah baik setiap 2 tahun, yang juga berkait rapat dengan tamat tempoh sah suatu sijil tandatangan digital. ii) Perlu juga dimaklumi bahawa isu-isu berkaitan kriptografi telah diperhalusi dalam dokumen **Rangka Kerja Prasarana Kunci Awam Kerajaan** yang diterbitkan pada

		tahun 2016 dan kepunyaan MAMPU. Dokumen ini boleh dijadikan dokumen rujukan awalan kepada inisiatif ini.
7-12	i) Melaksanakan tender terbuka untuk mendapatkan pembekal yang dipilih khas. ii) Melaksanakan proses menerima kertas cadangan dana penyelidikan khas untuk membangunkan prasarana kriptografi bergred tinggi.	Perlu melalui prosedur tender dan memberi dana penyelidikan yang terbuka dan telus.
13-15	i) Memilih pembekal yang bersesuaian. ii) Memilih penyelidikan yang bersesuaian.	Perlu melalui prosedur tender dan memberi dana penyelidikan yang terbuka dan telus.
16-28	i) Melaksanakan aktiviti tender (fasa pemantauan rapi). ii) Melaksanakan penyelidikan (fasa pemantauan rapi).	Memastikan hala tuju seperti yang ditetapkan. Kemungkinan untuk menamatkan pemberian tender atau dana penyelidikan jika tidak memenuhi jangkaan tujuan dana.
29-41	Menyiapkan aktiviti tender dan penyelidikan.	Memastikan aktiviti pemantauan berlaku dengan ketat.
42-45	Dokumentasi dan User Acceptance Test (UAT).	Memastikan proses menerima dokumentasi dan UAT berlaku dengan ketat.
46-48	Penyerahan produk kriptografi bergred tinggi kepada kerajaan.	Melancarkan produk kriptografi bergred tinggi untuk kegunaan Malaysia.

20. KESIMPULAN

Laporan ini mengandungi maklumat umum berkenaan kriptografi dan situasi semasa di Malaysia. Untuk menjayakan penggunaan kriptografi yang menyeluruh, suatu pendekatan dari peringkat tertinggi kerajaan perlu dilaksanakan. Kriptografi yang merupakan pertahanan terakhir keselamatan data negara perlu ada pertanggungjawaban dari pihak tertinggi. Yakni konsep pemilik keseluruhan maklumat negara. Ianya perlu berpaksi kepada suatu entiti yang secara konsepnya merupakan empunya semua data negara. Amalan memastikan

keselamatan maklumat terjamin dengan pelbagai jenis metodologi yang berpaksikan kepada amalan komersial tidak sesuai dalam usaha untuk menjayakan agenda e-kedaulatan. Hanya dengan metodologi satu pusat pertanggungjawaban akan dapat memastikan semua data Malaysia berada dalam keadaan selamat dalam satu tatacara yang piawai.