Persediaan menghadapi era kuantum

PETALING JAYA – Kemunculan era kuantum sedang mengubah cara dunia berfikir tentang keselamatan digital. Komputer kuantum yang dibangunkan oleh kuasa besar dunia mampu melakukan pengiraan amat rumit dalam tempoh masa singkat, sesuatu yang mustahil dicapai oleh komputer konvensional.

Keupayaan ini menimbulkan kebimbangan besar kerana ia berpotensi memecahkan sistem penyulitan data sedia ada yang selama ini menjadi benteng utama perlindungan maklumat global.

Dalam konteks ini, ancaman terhadap sistem keselamatan maklumat tidak lagi bersifat teori. Beberapa algoritma penyulitan tradisional seperti RSA dan ECC yang digunakan secara meluas dalam transaksi digital, komunikasi kerajaan dan sistem kewangan kini dianggap berisiko tinggi.

Dunia perlu bersiap sedia bukan sahaja dari segi pembangunan teknologi baharu, tetapi juga dari sudut dasar dan tadbir urus bagi memastikan peralihan kepada sistem keselamatan baharu berjalan dengan selamat dan teratur.

Perlindungan utama terhadap ancaman ini dikenali sebagai Kriptografi Pasca-Kuantum (*Post-Quantum Cryptography*, PQC), sistem kriptografi yang direka untuk menahan serangan komputer kuantum.

Di peringkat antarabangsa, badan seperti National Institute of Standards and Technology (NIST) di Amerika Syarikat, European Telecommunications Standards Institute (ETSI), dan International Organization for Standardization (ISO) sedang membangunkan serta menyelaras standard global bagi pelaksanaan PQC.

PERSIDANGAN dan Pameran Antarabangsa Teknologi PQC bakal diadakan di Pusat Kebudayaan dan Kesenian Sultan Salahuddin Abdul Aziz Shah, UPM pada 12-13 November ini.

> Pusat Teknologi dan Pengurusan Kriptologi Malaysia (PTPKM) memainkan peranan penting melalui Bahagian Polisi dan Pematuhan untuk memperkukuh tadbir urus kriptografi negara.

Walaupun kemajuan teknikal semakin pantas, kesiapsiagaan dari segi dasar dan polisi masih menjadi cabaran utama. Malaysia misalnya, walaupun telah mewujudkan Dasar Kriptografi Negara, rangka kerja khusus untuk pelaksanaan PQC masih dalam pembangunan.

Ketiadaan garis panduan yang menyeluruh boleh menyebabkan ketidaksamaan dalam pemilihan algoritma, pengurusan kunci, prosedur perolehan serta pematuhan audit antara agensi kerajaan dan sektor industri.

Pusat Teknologi dan Pengurusan Kriptologi Malaysia (PTPKM) memainkan peranan penting melalui Bahagian Polisi dan Pematuhan untuk memperkukuh tadbir urus kriptografi negara.

Ia kini sedang menggubal polisi, panduan dan rangka kerja pelaksanaan bagi menyokong penerapan PQC di pelbagai sektor strategik negara.

Ini termasuk penyediaan dokumen penting seperti rangka kerja tadbir urus teknologi maklumat dan komunikasi (ICT), pelan kesinambungan perkhidmatan (PKP) serta piawaian pematuhan perolehan yang mengambil kira keperluan keselamatan pasca-kuantum.

Selain itu, PTPKM membantu agensi Infrastruktur Maklumat Kritikal Negara (NCII) dalam melaksanakan Penilaian Risiko Kuantum.

Proses ini membantu agensi mengenal pasti sistem yang masih menggunakan kriptografi kunci awam, menilai tahap risiko, dan merancang pelan tindakan untuk mengurangkan ancaman masa depan, selain mengelak risiko *Harvest Now, Decrypt Later* iaitu taktik mencuri maklumat hari ini untuk dinyah sulit apabila komputer kuantum menjadi lebih berkuasa kelak.

Persediaan menghadapi era kuantum menuntut kerjasama menyeluruh antara kerajaan, industri, akademik dan rakan antarabangsa.

Melalui peranan PTPKM sebagai pusat penyelidikan kriptografi negara dan dengan sokongan dasar yang jelas serta fleksibel, Malaysia berada pada landasan kukuh untuk membina sistem keselamatan kriptografi yang berdaya tahan, selamat dan bersedia menghadapi cabaran dunia digital masa hadapan.