Nieuws

AIVD, CWI en TNO komen met vernieuwd handboek quantumveilige encryptie

dinsdag 3 december 2024, 13:23 door **Redactie**, 0 **reacties**

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Centrum Wiskunde & Informatica (CWI) en TNO hebben een **vernieuwd handboek** voor de overstap naar quantumveilige encryptie gepubliceerd. Ruim anderhalf jaar geleden verscheen de **eerste editie**. De tweede editie bevat onder andere concreter advies voor het vinden van cryptografische componenten, het beoordelen van quantumrisico's en het inrichten van 'cryptografische wendbaarheid'.

Quantumcomputers zullen volgens experts tussen 2030 en 2040 waarschijnlijk over voldoende rekenkracht beschikken om veel van de meest gebruikte encryptie-algoritmes te kraken. Hoewel "Q-Day" nog volgens deze inschattingen jaren verwijderd is, bestaat nu al het risico dat aanvallers versleutelde data onderscheppen om die op een later moment met een quantumcomputer te kraken. De Amerikaanse overheid waarschuwde onlangs nog dat kwaadwillenden nu al bezig zijn met een '**store now - decrypt later**' strategie.

Het overstappen naar een nieuw encryptie-algoritme kan lang duren. "Vandaar dat organisaties die werken met belangrijke versleutelde informatie – zoals staats- of bedrijfsgeheimen - nu al bezig moeten zijn met de overstap naar een quantumveilige omgeving", aldus de AIVD. Het handboek moet organisaties helpen om risico's te identificeren en te werken aan een migratiestrategie, waarbij gebruik wordt gemaakt van de kennis die sinds de eerste druk is opgedaan. Het handboek volgt een driestappenplan om de quantumdreiging te mitigeren: diagnose van quantumkwetsbaarheid, planning en uitvoering.

De AIVD, CWI en TNO adviseren organisaties om nu al te beginnen met een zogenaamde cryptografische inventarisatie, om tot een overzicht te komen van welke cryptografie er allemaal gebruikt wordt. Verder worden er in het handboek praktische ervaringen rondom de migratie gedeeld én bevat het de nieuwe adviestool **PQChoiceAssistant**, een opensourcetool die bedrijven moet helpen bij hun keuze van een Post-Quantum Cryptography (PQC) methode.

See below a table with general information on the available PQC algorithms. This page can be used in combination with the questionnaires to gain greater insight into the different PQC options. You can use the buttons at the top to switch between encryption (encapsulation) algorithms and signature algorithms, and also to switch to a visual comparison between the algorithms.

Characteristic	ML-KEM	FrodoKEM	Classic McEliece	BIKE	HQC
1 Underlying hard problem	Based on the module learning with errors problem (lattice-based)	Based on the learning with errors problem (lattice-based)	Based on the decoding of Goppa codes (code-based)	Based on quasi-cyclic moderate density parity-check (code-based)	Based on the Syndrome Decoding problem (code-based)
2 Maturity	Published in 2017	Published in 2016	First version published in 1978	Published in 2018	Published in 2017
3 Standardisation	Won NIST's six-year long competition and was selected as its main standard in 2024; also in the process of being standardised by ISO	Selected as an alternate candidate by NIST, but not selected for standardisation; is in the process of being standardised by ISO	Still in competition - has been selected for NIST standardisation round 4; also in the process of being standardised by ISO	Still in competition - has been selected for NIST standardisation round 4	Still in competition - has been selected for NIST standardisation round 4
4 Key issues	-	-	-	Has possible decryption failures, related to performance	-

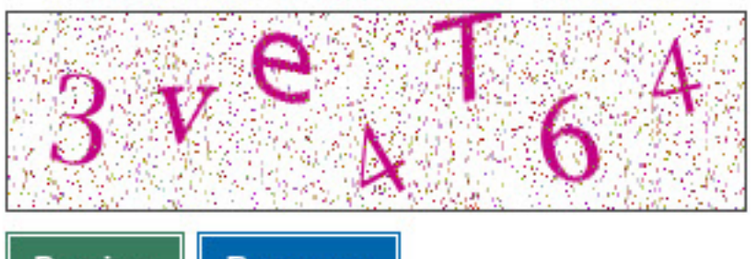
Politie haalt chatdienst Matrix uit de lucht en kon maandenlang meelezen
Banken blokkeerden vorig jaar ruim vijfduizend rekeningen wegens fraude

Nog geen reacties

Reageren

Ondersteunde bbcodes

Je bent niet ingelogd en reageert "**Anoniem**". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt **niet direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt kun je hier direct een account aanmaken. Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.



Nieuwe code

Herhaal code:

Preview Reageren