**Ministeren for videnskab, teknologi og udvikling**

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

Hermed fremsendes i 5 eksemplarer svar på spørgsmål nr. UVT alm. del-spørgsmål 1 (Alm. del - bilag ) stillet af Udvalget for Videnskab og Teknologi den 25. februar 2005.

Med venlig hilsen

Helge Sander

**Ministeriet for Videnskab, Teknologi og Udvikling**
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

**Spørgsmål nr. UVT alm. del-spørgsmål 1 stillet af Udvalget for Videnskab og Teknologi den 25. februar 2005 til Ministeren for videnskab, teknologi og udvikling (Alm. del - bilag )**

**Spørgsmål UVT alm. del-spørgsmål 1**
Vil ministeren påbegynde udskiftningen af SHA-1 algoritmen i den Digitale Signatur på baggrund af de nyligt fremkomne sikkerhedsbrister, som kinesiske forskere har påpeget i SHA-1 og dermed i den Digitale Signaturs sikkerhed, at det nu er blevet muligt at knække krypteringsalgoritmen SHA-1, der sikrer datasikkerheden i den Digitale Signatur, ComON 16. februar 2005 http://www.comon.dk/index.php/show/id=21161

**Svar:**
En digital signatur består af to dele: en komprimeringsdel der beregner et slags fingeraftryk på en meddelelse og en underskriftsdel der krypterer meddelelsens "fingeraftryk". Algoritmen SHA-1 benyttes kun i komprimeringsdelen, og selve underskriftsdelen er ikke berørt af de nye resultater.

SHA-1 er en international udbredt standard, der anvendes af stort set alle de programmer (e-mail, browsere, dokumenthåndteringssoftware etc.), som brugerne anvender i forbindelse med digital signatur.

SHA-1 indgår således ved udstedelsen af OCES certifikatet, idet TDC som certifikatudbyder digitalt underskriver brugerens certifikat, og i mange andre leverandørers produkter (Microsoft, IBM, Appel, Novell etc.), som gør brug af OCES certifikaterne.

Tre kinesiske forskere har, efter hvad der er blevet offentliggjort, nu fundet en metode, som reducerer antallet af beregninger, der kræves for at bryde SHA-1. Normalt vil det i SHA-1 kræve 2 opløftet i 80. potens for at finde to matchende tekster med samme "fingeraftryk". Den metode, som de kinesiske forskere har fundet, reducerer det tal til 2 opløftet i 69. potens.

Der er endnu ikke officielt kommet detaljer frem, om den metode de kinesiske forskere har anvendt, og det vides derfor ikke om metoden fungerer i praksis.

På det oplyste grundlag er det Videnskabsminsteriets opfattelse, at kinesernes forskningsresultat ud fra en rent akademisk synsvinkel er et stort resultat og et væsentligt fremskridt inden for kryptografien, men i praksis betyder resultatet ikke at den digitale signatur er brudt.

2 opløftet i 69. potens beregninger er stadig virkelig mange beregninger, som kræver betydelig tid selv med nutidens regnekraft for computere. Derudover er det ikke blevet lettere, at finde to matchende tekster med et meningsgivende indhold, der i praksis vil kunne anvendes af en bedrager.

Dette bekræftes da også af officielle udtalelser fra såvel danske som udenlandske uafhængige eksperter på området:

- Bruce Schneier førende international sikkerhedsekspert: "For the average Internet user, this news is not a cause for panic. No one is going to be breaking digital signatures or reading encrypted messages anytime soon. The electronic world is no less secure after these announcements than it was before." (Weblog covering security den 18.02.05)

- Professor ved DTU Lars R. Knudsen: "De nye resultater fra Kina er meget imponerende. Men så må jeg også skynde mig at sige, at der altså er lang vej endnu, inden man kan snakke om, at den digitale signatur er knækket." (Comon den 17.02.05). Lars R. Knudsen understreger i samme artikel, at chancen for at finde to meddelelser med samme ”fingeraftryk”, som rent faktisk indeholder meningsfuld tekst på forståelig dansk, er forsvindende lille.

- Professor ved Århus Universitet Ivan Damgård: "Hidtil har man forventet, at det krævede et astronomisk stort antal operationer - to i 80. potens -, men kineserne har vist, at det kan gøre på to i 69. potens. Det er stort set lige så astronomisk og stadig for stort til at kunne udføres i praksis. Men det er et klart signal om, at man bør skifte funktionen ud." (Berlingske.dk den 21.02.05)

- Krypteringsekspert professor Peter Landrock: ”Det vil være forkert at sige, at den digitale signatur, OCES, er sårbar overfor det her angreb. Men det er et vink om, at funktionen bør skiftes ud, men uden at gå i panik.” (Computerworld Online den 17.02.05)



Det amerikanske standardiseringsinstitut, NIST, har tidligere anbefalet, at SHA-1 bør udfases inden 2010. Det må formodes, at denne tidshorisont vil blive fremrykket med de seneste resultater.

Det er i den forbindelse vigtig, at være opmærksom på, at et skift fra SHA-1 til andre algoritmer er et globalt anliggende.

Et isoleret skift af SHA-1 i TDC’s produkter vil ikke give mening, idet f.eks. e-mailklienter og browsere fra Microsoft, Appel, IBM, etc. samtidig skal kunne understøtte den nye algoritme, hvilket de ikke gør i dag. Det er den internationale it-industri og standardiseringsorganisationerne, der skal koordinere og sikre en flydende og problemfri overgang fra SHA-1 til en stærkere Hash-algoritme.

På det foreliggende grundlag har Videnskabsministeriet taget kontakt til TDC med henblik på at sikre, at TDC etablerer det fornødne beredskab, så TDC betids vil kunne foretage den nødvendige omlægning fra SHA-1 til en ny Hash-algoritme.

Videnskabsministeriet og TDC har derfor konkret aftalt, at TDC vil arbejde på en udfasning af SHA-1 efter følgende handlingsplan:

- TDC vil tæt følge analysen af de kinesiske forskningsresultater i forhold til at vurdere konsekvenserne heraf.

- TDC vil tæt følge standardiseringsorganisationernes anbefalinger om anvendelse af en ny Hash-algoritme og standardapplikationers understøttelse heraf.

- TDC vil etablere det fornødne beredskab og planlægning af tilpasninger i egne systemer med henblik på betids at kunne foretage en problemfri overgang til en ny Hash-algoritme.

- TDC vil udskifte til en nye Hash-algoritme, når den nye algoritme understøttes bredt af de gængse standardprogrammer.

- TDC vil løbende rapportere til Videnskabsministeriet om status på området.

Med forbehold for at der ikke fremkommer nye oplysninger i sagen, vurderer Videnskabsministeriet, at der med den aftalte plan er den nødvendige og tilstrækkelige fokusering på problemet.

**Ministeriet for Videnskab, Teknologi og Udvikling**