»Forskningsresultaterne fremlagt på årets Crypto konference i USA er et vidnesbyrd om, at der internationalt bruges mange kræfter på at analysere sikkerheden af de algoritmer, som blandt andet anvendes til OCES digital signatur i Danmark.

Selve forskningsresultatet giver ikke anledning til at ændre på noget i den eksisterende løsning i Danmark, men indikerer, at det indenfor en årrække sandsynligvis vil være nødvendig at vælge en afløser for SHA-1 algoritmen, som det tidligere er sket for andre algoritmer. Der er allerede standardiseret et antal andre algoritmer, der kandiderer til at blive den foretrukne afløser. TDC følger udviklingen nøje, således at OCES digital signatur kan skifte over til en ny algoritme, når den internationale sikkerhedsverden på et tidspunkt anbefaler dette.«

Jeg har til sagens yderligere oplysning indhentet følgende tekniske redegørelse:

»De omtalte algoritmer er såkaldte hash-algoritmer, der bruges når indholdet i et digitalt dokument skal sikres. Matematikken bag er, at algoritmen på basis af dokumentets indhold udregner en checksum. Sker der ændringer i dokumentet påvirkes checksummen, og ændringer af dokumenter kan dermed afsløres. Hash-algoritmerne har således til formål at sikre dokumentets integritet.

Hash-algoritmerne antages at have egenskaben, at det er så godt som umuligt at regne baglæns, dvs. skabe et falsk dokument som – når checksummen udregnes – giver samme resultat som det ægte dokument – en situation som betegnes hash-kollision.

MD5 og SHA-0 anvendes ikke i OCES digitale signaturer.

SHA-1 er udviklet af NSA og anerkendt globalt. SHA-1 anvendes over hele verden i mange forskellige kommunikationssystemer og produkter. SHA-1 indgår som en del af en OCES digital signatur, idet det er den af SHA-1 frembragte checksum der »underskrives digitalt«.

Styrken i klassiske krypteringsalgoritmer er baseret på, at det med den eksisterende tilgængelige computerkraft er uendelig svært eller ugørligt at bryde de krypterede koder. Dette gælder også SHA-1, idet det med den eksisterende tilgængelige computerkraft anses ugørligt at konstruere et dokument, der passer til en given checksum.

Det betyder, at alle krypteringsalgoritmer – herunder SHA-1 – har en tidsbegrænset holdbarhed. Efterhånden som computerkraften øges bliver algoritmerne forbedret eller udskiftet.

Endvidere arbejder krypteringsanalytikere løbende intensivt på at finde teoretiske svagheder i krypteringsalgoritmer, hvilket også medfører at algoritmerne over tid enten forbedres eller udskiftes. Dette er den normale proces i krypteringsanalytikernes verden, og processen er med til at sikre at algoritmerne løbende har en tilstrækkelige sikkerhedsstyrke. Efter at der blev konstateret teoretiske svagheder i hash-algoritmerne MD5 og SHA-0 i midten af 90'erne, er disse løbende blevet udskiftet med SHA-1.

På Crypto konferencen 2004 i Santa Barbara USA blev der så ført et bevis for, at det nu var muligt at bryde MD5 og SHA-0. Der blev endvidere ført bevis for, at der ud fra checksummen kunne konstrueres et dokument, når SHA-1 kun blev *partielt eksekveret*. Men SHA-1 kræver et gennemløb på 80 trin, og beviset blev ført for de første 40 trin.

Hertil kommer, at den teoretiske svaghed kun i praksis ville kunne udnyttes, hvis der *frit kunne vælges to tekster* henholdsvis to programmer, der giver den samme checksum. Dette vil under normale forhold ikke være tilfældet, hvorfor risikoen for forfalskning af læsbare tekster eller virusbefængte programmer ville være uendelig lille. Det ville således være usandsynligt, at der blot ville kunne ændres f.eks. et beløb eller indføje en virus i et program.

Konklusionen er, at der ikke er gennemført et vellykket angreb på SHA-1, men krypteringsanalytikere er kommet et skridt længere i bestræbelserne på at bryde SHA-1. Der er ingen der ved, hvornår krypteringsanalytikere tager et næste skridt på vejen til at kunne bryde SHA-1, men nye versioner af stærkere hash-algoritmer er allerede på vej.

Krypteringseksperter verden over er dog generelt enige om, at der ikke er grund til panik, idet angrebene kun er teoretiske, men at der fortsat skal holdes øje med udviklingen, så der betids vil kunne skiftes til en anden stærkere algoritme. Krypteringseksperten Bruce Schneier har f.eks. udtalt: »As a cryptographer, this is really interesting and exciting, but as a computer user there's no real reason to worry«.«

Jeg kan i øvrigt tilføje, at vi i Danmark har et forskningsmiljø i international klasse, der følger udviklingen og som kan sikre, at denne vigtige viden om kryptering bliver omsat til praktisk sikkerhed. Således er Aarhus Universitet vært