Het Selecteren van Cryptografische Sleutellengten in Commerciële Toepassingen[1]

Arjen K. Lenstra

Eric R. Verheul

1 Introductie

Cryptografische technieken zijn belangrijke bouwstenen voor de bescherming van informatie in electronic commerce toepassingen, met name voor de bescherming van de vertrouwelijkheid, integriteit, authenticiteit en onweerlegbaarheid van informatie. De uiteindelijke kwaliteit van deze bescherming hangt niet alleen af van de gebruikte cryptografische techniek en de gebruikte sleutellengten, maar met name van de wijze (protocol ontwerp) waarop de technieken worden ingezet.

In dit artikel geven we richtlijnen voor het bepalen van cryptografische sleutellengten, andere belangrijke zaken zoals protocol ontwerp bespreken we niet. Dit artikel is een samenvatting van [2], waar een gedetailleerde onderbouwing van onze richtlijnen wordt gegeven. Aanbevelingen inzake sleutellengten kunnen op talloze plaatsen worden gevonden, zoals in de cryptografische literatuur of in de documentatie van specifieke cryptografische producten. Helaas is het vaak moeilijk te bepalen waarop deze aanbevelingen zijn gebaseerd. Voorzover wij weten is dit het eerste artikel waarin dit onderwerp op een uniforme, reproduceerbare en goed gedocumenteerde wijze wordt benaderd. Onze richtlijnen stellen organisaties in staat een onderbouwd oordeel te vormen over sleutellengten bij de aanschaf of ontwikkeling van cryptografische applicaties. We hebben hierbij de belangrijkste cryptografische systemen als basis genomen, namelijk:

- Symmetrische sleutel systemen: zoals de Data Encryption Standard (DES).
- Klassieke asymmetrische (of publieke) sleutel systemen, dit zijn het RSA systeem en de traditionele discrete logaritme systemen, zoals ElGamal (Elg) en Diffie-Hellman (DH). Alle worden ondersteund in het populaire versleutelpakket “Pretty Good Privacy” (PGP).
- Subgroep discrete logaritme systemen: dit omvat bijvoorbeeld het US Digital Signature Algorithm (DSA), en het Schnorr digitale handtekening systeem.
- Elliptische Kromme systemen.

Behalve in brochures worden deze systemen ook in het Wassenaar Arrangement genoemd dat een export-vergunning stelsel realiseert. Hiermee tracht men de proliferatie van (krachtige) cryptografische producten te beperken. In de bijlage beschrijven we deze systemen op summiere wijze. Verder vermelden we daar de maximale sleutellengten uit het Wassenaar Arrangement die cryptografische producten mogen ondersteunen, wil er voor de export geen vergunning vereist zijn.

[1] Dit artikel is verschenen in het “Informatiebeveiliging Praktijkjournaal, Nr. 7, 1999, tenHagenStam, p.11-17.

Het is met enige aarzeling dat we deze richtlijnen voor sleutellengten geven. Vaak hebben organisaties die op zoek zijn naar een betrouwbaar systeem, meer oog voor de gebruikte cryptografische technieken en sleutellengten, dan voor het ontwerp waarmee deze technieken worden ingezet. In onze ervaring is het falen van cryptografische systemen bijna altijd het gevolg van een ontwerpfout binnen het gehele systeem, en niet van verkeerd gekozen cryptografische technieken of sleutellengten. Zie ook [1]. Met andere woorden, men kan zich beter eerst (laten) overtuigen van de kwaliteit van het ontwerp van het gehele systeem, dan dat men alleen naar de gebruikte technieken of sleutellengten kijkt. We noemen twee voorbeelden ter illustratie. De cryptografische technieken en sleutellengten die gebruikt worden binnen bovengenoemde PGP, zijn ruimschoots voldoende om bescherming te bieden voor informatie die verstuurd wordt over het Internet. Maar het wachtwoord dat de geheime PGP sleutels beschermt op de gebruikers PC, die in principe benaderbaar is vanuit het Internet, is dat veelal niet. Zelfs als de gebruiker erg beveiligingsbewust is en een willekeurig wachtwoord kiest van 8 karakters uit een verzameling van 128 mogelijkheden, dan nog is de geboden beveiliging vergelijkbaar met de beveiliging die geboden wordt door de recent gebroken “Data Encryption Standard”(DES), zie [3], en dus onacceptabel naar huidige normen. Een tweede voorbeeld is het gebruik van wachtwoorden binnen Windows NT Networking, waarbij wachtwoorden worden “versleuteld” bij transport over het netwerk, en waarbij gebruikers wachtwoorden mogen kiezen tot 14 karakters lengte, die onmogelijk te breken lijken te zijn. Echter, bij veel Windows NT Netwerk configuraties wordt bij de versleuteling het wachtwoord in twee stukken van 7 of minder karakters opgedeeld en afzonderlijk “versleuteld” en verstuurd over het netwerk. In de praktijk betekent dit dat de effectieve lengte van wachtwoorden slechts 7 of minder karakters is: absoluut onvoldoende naar de huidige normen.

Onze richtlijnen zijn gebaseerd op redelijke extrapolaties van ontwikkelingen uit de laatste twee decennia. Deze benadering kan falen. Zoals ook in het verleden is gebleken, kan een enkel briljant idee bewijzen dat een cryptografische techniek aanzienlijk minder veilig is dan gedacht.

De opzet van dit artikel is als volgt:

- In Sectie 2 beschrijven we het door ons ontwikkelde model voor de bepaling van sleutellengten.
- In Sectie 3 bespreken we de resultaten van het model en de consequenties hiervan.
- In Sectie 4 plaatsen we enkele kantekeningen bij ons model.

2 Het Model

Zodra men voldoende overtuigd is van de kwaliteit van het ontwerp van een systeem, d.w.z. dat het systeem alleen gecompromitteerd kan worden door een rechtstreekse aanval op de gebruikte cryptografische technieken, moet men een keuze gaan maken inzake sleutellengten. Deze keuze hangt primair af van de volgende drie, nader te kwantificeren, parameters:

I. Levensduur: de verwachte tijd dat de informatie beschermd moet worden tegen aanvallers.

II. Beschermingsdrempel: een acceptabele mate van zekerheid dat aanvallen door aanvallers tijdens de levensduur van de informatie niet uitvoerbaar zijn. Dit hangt met name af van *wie* de aanvallers zijn en over hoeveel rekenkracht en financiën ze kunnen beschikken voor de aanval.

III. Cryptanalyse: de effectiviteit van aanvallen tijdens de levensduur van de informatie.

2.1 Levensduur

Dit is de cruciale parameter binnen ons model, en het is de verantwoordelijkheid van de organisatie zelf om te kwantificeren tot welk jaar informatie beschermd moet worden.

2.2 Beschermingsdrempel

Het is in de praktijk erg moeilijk om te bepalen wie de aanvallers van een organisatie en van diens informatie zijn. Het is al helemaal moeilijk te bepalen wat de capaciteiten van de onderkende aanvallers zijn. Daarmee is het kwantificeren van een beschermingsdrempel op deze wijze praktisch onmogelijk. Wij kiezen voor een andere benadering, waarbij we een beschermingsdrempel kiezen uit het verleden en deze, met behulp van twee andere hypothesen, naar de toekomst extrapoleren.

Hypothese I.
Als basis voor een beschermingsdrempel nemen we aan dat de "Data Encryption Standard" (DES) voldoende bescherming bood voor commerciële applicaties tot 1982. De DES standaard werd geïntroduceerd in 1977 en in de standaard was opgenomen dat de standaard iedere vijf jaar, na een nieuwe beoordeling, moest worden verlengd. We nemen daarom aan dat de benodigde reken-inspanning ('computational effort') om DES te breken een voldoende beschermingsdrempel bood voor commerciële applicaties tot 1982.

De reken-inspanning benodigd om DES te breken is geschat op $5 * 10^5$ Mips Jaren, zie [2]. De eenheid *Mips Jaar* representeert de hoeveel berekeningen die kunnen worden uitgevoerd in 1 jaar op een enkele VAX 780, en is ruwweg equivalent met 20 uur op een 450MHz PentiumII processor. Dus, $5 * 10^5$ Mips Jaren is ongeveer 14000 maanden op een 450MHz PentiumII processor, of 2 maanden op 7000 van zulke processors. Omdat computers sneller en goedkoper zijn geworden in de loop der jaren, moet deze reken-inspanning geëxtrapoleerd worden naar het heden en de toekomst. Hiervoor hebben we een tweede hypothese, namelijk Moore's Wet.

Hypothese II.
Een wereldwijd geaccepteerde interpretatie van Moore's Wet stelt dat de rekenkracht die men krijgt van een chip elke 18 maanden verdubbelt, met het uitkomen van nieuwe typen. Men is enigszins sceptisch over de geldigheid van deze wet, omdat op een gegeven moment essentieel nieuwe technieken moeten worden uitgevonden. Mede hierom kiezen wij voor een variant van Moore's Wet die minder technologie afhankelijk is en die tot nu toe voldoende accuraat is: de hoeveelheid rekenkracht die men krijgt voor een dollar verdubbelt iedere 18 maanden. Het volgt aldus dat men iedere 10 jaar een factor $2^{10*12/18} \approx 100$ meer rekenkracht krijgt voor dezelfde hoeveelheid geld.

Hypothese III. Onze versie van Moore's Wet impliceert dat we ook budget toenamen van organisaties moeten meenemen in onze beschouwingen. Het Bruto Nationaal Product van de VS laat iedere tien jaar een verdubbeling zien: $1630 miljard in 1975, $4180 miljard in 1985, en $7269 miljard in 1995. Dit brengt ons tot de hypothese dat het budget van organisaties – ook van organisaties die cryptografische systemen breken – iedere 10 jaar verdubbelt.

Illustratie: combinatie van Hypothesen I, II, en III.

Als $5*10^5$ Mips Jaren in 1982 een voldoende beveiligingsdrempel was voor commerciële applicaties, dan is $1*10^8$ ($\approx 2*100*5*10^5$) Mips Jaren dat in 1992 en is $2*10^{10}$ ($\approx 200*1*10^8$) Mips Jaren dat in 2002, en $4*10^{12}$ Mips Jaren in 2012.

2.3 Cryptanalyse

Hypothesis IV.

Voor alle vier de cryptografische systemen die we als basis hebben genomen in dit artikel zijn aanvallen bekend in de cryptografische literatuur. Aan de hand van de complexiteit van deze aanvallen zijn we in staat voor elk van de vier onderscheiden cryptografische systemen een relatie te leggen tussen sleutellengten en reken-inspanning en dus met beschermingsdrempels. Voor details verwijzen we naar [2].

Het is onmogelijk om aan te geven welke cryptografische progressie er plaats zal vinden in de toekomst. Wij vinden het echter redelijk om aan te nemen dat deze progressie niet veel zal verschillen met de progressie die plaatsgevonden heeft tussen 1970 en 1999. Voor klassieke asymmetrische systemen lijkt deze progressie erg op het effect van Moore's Wet. Dat wil zeggen, elke 18 maanden verwachten we dat een aanval op een klassiek asymmetrisch systeem slechts de helft van de huidige rekenkracht kost. Voor de andere typen cryptografische systemen nemen we aan dat er geen substantiële cryptanalytische ontwikkelingen zullen plaatsvinden, met de uitzondering van cryptografische systemen gebaseerd op Elliptische Krommen. Hier zullen we twee aparte typen extrapolaties toepassen: geen progressie en progressie à la Moore.

3 De resultaten van het model

Binnen ons model kunnen we nu op redelijk eenvoudige wijze suggesties doen voor sleutellengten op basis van de levensduur. Immers, met behulp van de levensduur en de hypothesen kan de beschermingsdrempel in Mips Jaren worden bepaald die de informatie moet krijgen van de cryptografische techniek. Eveneens aan de hand van de levensduur en aan de hand van hypothese IV, kan voor alle onderscheiden cryptografische systemen worden bepaald met welke sleutellengte deze beschermingdrempel correspondeert. Deze sleutellengten zijn geplaatst in onderstaande tabel 1.

Tabel 1

Gesuggereerde ondergrenzen voor sleutellengten in bits, uitgaande van cryptanalytische progressie à la Moore bij klassieke asymmetrische systemen

Year	Sym-metrische Sleutel Lengte (bits)	Klassieke Asym-metrische Sleutel Lengte (RSA, Elg DH) (bits)	Subgroep Discrete Logaritme Sleutel Lengte (DSA, Schnorr) (bits)	Elliptisch Kromme Sleute Lengte (in bits)		Beschermings Drempel (Mips Jaren)	Correspond. aantal jaren op 450MHz PentiumII PCs	Correspond. Budget voor een aanval in 1 dag (dollars)
				Progress				
				no	Yes			
1982	56	417	102	105		$5.00 * 10^5$	$1.11 * 10^3$	$3.98 * 10^7$
1985	59	488	106	110		$2.46 * 10^6$	$5.47 * 10^3$	$4.90 * 10^7$
1990	63	622	112	117		$3.51 * 10^7$	$7.80 * 10^4$	$6.93 * 10^7$
1995	66	777	118	124		$5.00 * 10^8$	$1.11 * 10^6$	$9.81 * 10^7$
2000	70	952	125	132	132	$7.13 * 10^9$	$1.58 * 10^7$	$1.39 * 10^8$
2001	71	990	126	133	135	$1.21 * 10^{10}$	$2.70 * 10^7$	$1.49 * 10^8$
2002	72	1028	127	135	139	$2.06 * 10^{10}$	$4.59 * 10^7$	$1.59 * 10^8$

2003	73	1068	129	136	140	$3.51 * 10^{10}$	$7.80 * 10^{7}$	$1.71 * 10^{8}$
2004	73	1108	130	138	143	$5.98 * 10^{10}$	$1.33 * 10^{8}$	$1.83 * 10^{8}$
2005	74	1149	131	139	147	$1.02 * 10^{11}$	$2.26 * 10^{8}$	$1.96 * 10^{8}$
2006	75	1191	133	141	148	$1.73 * 10^{11}$	$3.84 * 10^{8}$	$2.10 * 10^{8}$
2007	76	1235	134	142	152	$2.94 * 10^{11}$	$6.54 * 10^{8}$	$2.25 * 10^{8}$
2008	76	1279	135	144	155	$5.01 * 10^{11}$	$1.11 * 10^{9}$	$2.41 * 10^{8}$
2009	77	1323	137	145	157	$8.52 * 10^{11}$	$1.89 * 10^{9}$	$2.59 * 10^{8}$
2010	78	1369	138	146	160	$1.45 * 10^{12}$	$3.22 * 10^{9}$	$2.77 * 10^{8}$
2011	79	1416	139	148	163	$2.47 * 10^{12}$	$5.48 * 10^{9}$	$2.97 * 10^{8}$
2012	80	1464	141	149	165	$4.19 * 10^{12}$	$9.32 * 10^{9}$	$3.19 * 10^{8}$
2013	80	1513	142	151	168	$7.14 * 10^{12}$	$1.59 * 10^{10}$	$3.41 * 10^{8}$
2014	81	1562	143	152	172	$1.21 * 10^{13}$	$2.70 * 10^{10}$	$3.66 * 10^{8}$
2015	82	1613	145	154	173	$2.07 * 10^{13}$	$4.59 * 10^{10}$	$3.92 * 10^{8}$
2016	83	1664	146	155	177	$3.51 * 10^{13}$	$7.81 * 10^{10}$	$4.20 * 10^{8}$
2017	83	1717	147	157	180	$5.98 * 10^{13}$	$1.33 * 10^{11}$	$4.51 * 10^{8}$
2018	84	1771	149	158	181	$1.02 * 10^{14}$	$2.26 * 10^{11}$	$4.83 * 10^{8}$
2019	85	1825	150	160	185	$1.73 * 10^{14}$	$3.85 * 10^{11}$	$5.18 * 10^{8}$
2020	86	1881	151	161	188	$2.94 * 10^{14}$	$6.54 * 10^{11}$	$5.55 * 10^{8}$
2021	86	1937	153	163	190	$5.01 * 10^{14}$	$1.11 * 10^{12}$	$5.94 * 10^{8}$
2022	87	1995	154	164	193	$8.52 * 10^{14}$	$1.89 * 10^{12}$	$6.37 * 10^{8}$
2023	88	2054	156	166	197	$1.45 * 10^{15}$	$3.22 * 10^{12}$	$6.83 * 10^{8}$
2024	89	2113	157	167	198	$2.47 * 10^{15}$	$5.48 * 10^{12}$	$7.32 * 10^{8}$
2025	89	2174	158	169	202	$4.20 * 10^{15}$	$9.33 * 10^{12}$	$7.84 * 10^{8}$
2026	90	2236	160	170	205	$7.14 * 10^{15}$	$1.59 * 10^{13}$	$8.41 * 10^{8}$
2027	91	2299	161	172	207	$1.21 * 10^{16}$	$2.70 * 10^{13}$	$9.01 * 10^{8}$
2028	92	2362	162	173	210	$2.07 * 10^{16}$	$4.59 * 10^{13}$	$9.66 * 10^{8}$
2029	93	2427	164	175	213	$3.52 * 10^{16}$	$7.81 * 10^{13}$	$1.04 * 10^{9}$
2030	93	2493	165	176	215	$5.98 * 10^{16}$	$1.33 * 10^{14}$	$1.11 * 10^{9}$
2031	94	2560	167	178	218	$1.02 * 10^{17}$	$2.26 * 10^{14}$	$1.19 * 10^{9}$
2032	95	2629	168	179	222	$1.73 * 10^{17}$	$3.85 * 10^{14}$	$1.27 * 10^{9}$
2033	96	2698	169	181	223	$2.95 * 10^{17}$	$6.55 * 10^{14}$	$1.37 * 10^{9}$
2034	96	2768	171	182	227	$5.01 * 10^{17}$	$1.11 * 10^{15}$	$1.46 * 10^{9}$
2035	97	2840	172	184	230	$8.53 * 10^{17}$	$1.90 * 10^{15}$	$1.57 * 10^{9}$
2036	98	2912	173	185	232	$1.45 * 10^{18}$	$3.22 * 10^{15}$	$1.68 * 10^{9}$
2037	99	2986	175	186	235	$2.47 * 10^{18}$	$5.49 * 10^{15}$	$1.80 * 10^{9}$
2038	99	3061	176	188	239	$4.20 * 10^{18}$	$9.33 * 10^{15}$	$1.93 * 10^{9}$
2039	100	3137	178	189	240	$7.14 * 10^{18}$	$1.59 * 10^{16}$	$2.07 * 10^{9}$
2040	101	3214	179	191	244	$1.22 * 10^{19}$	$2.70 * 10^{16}$	$2.22 * 10^{9}$

4 Consequenties van het model

Gebruik van de tabel

Indien men onze hypothesen accepteert, dan kan tabel 1 als volgt worden gebruikt voor de selectie van sleutellengten. Stel dat men een commerciële applicatie ontwikkelt waarbij de vertrouwelijkheid of integriteit van de informatie 20 jaar beschermd moet worden, d.w.z tot het jaar 2020. Uit de rij voor het jaar 2020 in tabel 1, kan men nu vaststellen dat $2.94 * 10^{14}$ Mips Jaren gezien kan worden als een voldoende beschermingsdrempel voor deze informatie en dat men de volgende sleutellengten moet overwegen:

- Symmetrische sleutels van **minstens** 86 bits;
- RSA moduli van **minstens** 1881 bits;
- Subgroep discrete logaritmen systemen met groep priemgetallen van **minstens** 151 bits en basis priemgetallen van **minstens** 1881 bits.
- Elliptische kromme systemen van **minstens** 161 bits als men er vertrouwen in heeft dat er geen cryptanalytische progressie zal plaatsvinden op dit terrein, en **minstens** 188 bits als men voorzichtiger wil zijn.

Consequenties voor de US Digital Signature Standard/Algorithm

De Amerikaanse standaard voor digitale handtekeningen (DSS/DSA) is gebaseerd op

een Subgroep Discrete Logaritme systeem, waarbij 160-bit subgroepen worden gebruikt in combinatie met een basis priemgetal p tussen de 512 en 1024 bits. Het volgt uit onze tabel dat de veiligheid die DSS/DSA biedt, twijfelachtig is na het jaar 2002. Omdat digitale handtekeningen geruime tijd na tekening betrouwbaar moeten zijn, is dit niet acceptabel. Als digitale handtekeningen betrouwbaar moeten zijn tot het jaar 2026, dan blijkt uit de tabel dat men beter DSA kan gebruiken met 2236-bit basis priemgetallen (aanzienlijk groter is dan het DSA maximum van 1024 bits). De lengte van de handtekening wordt hierdoor overigens niet langer.

Consequenties voor Internationale versies van SSL
Een populair protocol voor de uitwisseling van vertrouwelijke informatie (bijv. creditcard nummers) tussen een webbrowser (=klant) en webserver (= electronic commerce winkelier) is het Secure Sockets Layer (SSL) protocol. SSL maakt gebruikt van een RSA sleutel, geplaatst op de webserver (Microsoft Internet Information Server, Netscape Enterprise Server, Apache). Deze sleutel is veelal in certificaat vorm (d.w.z. getekend door een Certificate Authority). Met deze RSA sleutel wordt een sessiesleutel tussen webbrowser en webserver uitgewisseld, waarmee vervolgens vertrouwelijke informatie symmetrisch wordt versleuteld. Alleen als zowel de sessiesleutel als de RSA modulus groot genoeg zijn, ontstaat dus een veilige verbinding tussen browser en server.

Als gevolg van het Wassenaar arrangement, gebruiken internationaal beschikbare versies van web**browsers** sessiesleutels van slechts 40 bits lengte. Dit is onvoldoende naar huidige normen (komt niet eens voor in tabel 1). In internationaal beschikbare versies van de web**servers** (veelal gebruikt in Europa) worden RSA moduli van slechts 512-bit lengte gebruikt. Ook dit is onvoldoende naar huidige normen. Immers, indien een aanvaller deze SSL RSA sleutel breekt, dan is hij in staat om toegang te krijgen tot alle sessiesleutels en dus tot alle informatie die daarmee versleuteld wordt. Ondanks het feit dat uit onze tabel volgt dat 512-bit RSA moduli reeds in 1990 onvoldoende veilig waren, worden internationale versies van webservers en dus ook 512-bit RSA moduli nog veel gebruikt. In 1999 zijn in de wetenschappelijk wereld de eerste stappen gezet voor de factorisatie van een 512-bit RSA modulus. Dit heeft 22 augustus 1999 daadwerkelijk geleid tot de eerste factorisatie van een 512-bit RSA modulus. Behalve directe veiligheidrisico's zijn er dus nu ook aanzienlijke publicitaire risico's verbonden aan het gebruik van 512-bit RSA moduli. Immers, organisaties die ze gebruiken kunnen negatief in het nieuws komen nu in de media is gesuggereerd dat "512-bit RSA moduli" onveilig zijn.

De limiet genoemd in het Wassenaar Arrangement voor symmetrische versleuteling is 64 bit hetgeen meer bescherming biedt dan de 56 bit van DES. Uit bovenstaande tabel volgt dat vandaag de dag, de veiligheid van 64 bit symmetrische versleuteling ongeveer equivalent is met de veiligheid geboden door 768 bit RSA. Het zou daarom consistent zijn als de limiet in het Wassenaar Arrangement voor RSA sleutels op 768 bits zou worden gesteld. Dit zou de bescherming die internationale implementaties van SSL bieden, significant kunnen verhogen.

Voor Amerikaanse ("Domestic") webservers die veiliger sleutellengten gebruiken (zeg 1024 bit) is een Amerikaanse export vergunning vereist. Vroeger konden slechts bancaire instellingen zo'n vergunning krijgen, heel recent kunnen ook verzekeringsinstellingen, medische instanties en "on-line merchants" – in principe - een export vergunning krijgen voor een "domestic" webserver.

5 Een Kanttekening: Software versus hardware aanvallen

Men zou kunnen opwerpen dat we als maat voor de beschermingdrempel slechts het aantal benodigde Mips Jaren hebben genomen en daarmee de mogelijkheden van speciaal ontwikkelde kraak-hardware niet hebben meegenomen in onze beschouwingen. Echter, aan de hand van concrete voorbeelden (zie [2]), kunnen we aannemelijk maken dat ook de mogelijkheden van speciaal ontwikkelde kraak-hardware aan Moore's Wet voldoet. Met andere woorden, als men aanneemt dat DES voldoende bestand was tegen aanvallen met speciaal ontwikkelde kraak-hardware in 1982, dan blijft dat gelden voor de sleutellengten gesuggereerd voor de toekomst.

Dr. Arjen K. Lenstra werkt bij de afdeling Emerging Technologies van het Corporate Technology Office van Citibank in New York. Dr. Lenstra is een internationaal erkend expert op het gebied van cryptanalyse. Zo werd bijvoorbeeld zijn software gebruikt voor het kraken van de bekende 'RSA-129 challenge'.
Email: **Arjen.Lenstra@citicorp.com**

Dr. Eric R. Verheul, is werkzaam bij PriceWaterhouseCoopers te Utrecht en adviseert over informatiebeveiliging bij met name nieuwe E-commerce toepassingen. Eric is wetenschappelijk actief in de cryptologie, zowel in zijn theorie als zijn toepassingen. Verder doceert Eric aan de TU Eindhoven over informatiebeveiliging.
Email: **Eric.Verheul@nl.pwcglobal.com**

Referenties

[1] Why Cryptosystemen fail, R.J. Anderson, Communications of the ACM, v. 37, n.11, nov. 1994, pp. 32-40.
[2] Selecting Cryptographic Key Sizes, A.K. Lenstra, E.R. Verheul, in voorbereiding.
[3] Cracking DES, Electronic Frontier Foundation, O'Reilly, juli 1998.

6 Bijlage: een summiere beschrijving van de cryptografische systemen

De Coordinating Committee for Multilateral Export Controls (COCOM) was een internationale organisatie die de export van strategische producten, waaronder cryptografische, van aangesloten landen naar landen die hun nationale veiligheid bedreigden reguleerde. Aangesloten landen, onder meer Europese landen en de VS, implementeerden de COCOM regels in nationale wetgeving. Het Wassenaar Arrangement is een follow-up van de COCOM regels. De huidige beperkingen van cryptografie in het Wassenaar Arrangement zijn redelijk gedetailleerd. Van 4 typen cryptografische systemen worden de maximale sleutellengten genoemd waarbij export kan plaatsvinden zonder vergunning. Ook in dit artikel beperken we ons tot dit viertal. Naar de aard van het Wassenaar Arrangement is het weinig verrassend dat de genoemde sleutellengten onvoldoende bescherming bieden in de meerderheid van commerciële applicaties.

We onderscheiden de cryptografische systemen in symmetrische (‘geheime’) en asymmetrische (‘publieke’) sleutel systemen. Zulke systemen zijn belangrijke bouwstenen in electronic commerce applicaties, en kunnen gebruikt worden voor de waarborg van vertrouwelijkheid, integriteit, authenticiteit en onweerlegbaarheid van digitale informatie. Voor de eenvoud beschouwen we twee communicerende partijen, een verstuurder V en ontvanger O, die de vertrouwelijkheid van hun communicatie willen garanderen.

Symmetrische sleutel systemen

Beschrijving. Bij symmetrische sleutel systemen delen V en O een sleutel. Om de vertrouwelijkheid te garanderen, moet de vertrouwelijkheid van deze sleutel gewaarborgd zijn. De cruciale parameter bij symmetrische systemen is de sleutellengte, d.w.z. het aantal bits. Deze hangt af van het type symmetrische systeem. Het bekendste symmetrische systeem is de Data Encryption Standard (DES), geïntroduceerd in 1977, met een sleutellengte van 56 bits. Andere voorbeelden zijn:

- Three Key Triple DES (sleutellengte 168, effectieve sleutellengte 112);
- IDEA (sleutellengte 128);
- RC5 (variabele sleutellengte);
- De toekomstige opvolger van DES, de Advanced Encryption Standard (AES), met sleutellengten van 128, 192, of 256 bits.

Wassenaar Arrangement. De maximum symmetrische sleutellengte toegestaan door het Wassenaar Arrangement is 56 bits voor ‘niche market’ toepassingen en 64 bits for ‘mass market’ toepassingen. De reden voor dit verschil in sleutellengten laat zich raden.

Asymmetrische sleutel systemen

Bij asymmetrische sleutel systemen heeft de ontvanger O een private sleutel (die hij geheim houdt) en een corresponderende publieke sleutel waar iedereen, onder meer de verstuurder V, beschikking over heeft. De verstuurder V gebruikt de publieke sleutel van O om informatie te versleutelen bedoeld voor O, en deze gebruikt zijn private sleutel om de versleutelde informatie te ontsleutelen. Als de private sleutel afgeleid kan worden uit de publieke, dan kan het systeem gebroken worden.

Hoe de private en publieke sleutels gevormd worden en hoe moeilijk het is om het systeem te breken hangt af van het type systeem. Om cryptografische en historische redenen onderscheiden we drie soorten asymmetrische systemen:

- Klassieke asymmetrische systemen
- Subgroep discrete logaritme systemen
- Elliptische kromme discrete logaritme systemen, of simpelweg Elliptisch kromme systemen

Klassieke asymmetrische systemen

Hiermee worden RSA en de traditionele discrete logaritme (TDL) systemen bedoeld.

Bij RSA omvat de publieke sleutel een groot getal, de zogenaamde RSA modulus, dat bestaat uit het product van twee grote priemgetallen. Hoe asymmetrische versleuteling werkt, valt buiten de scope van dit artikel. Als deze priemgetallen teruggevonden kunnen worden uit hun product, dan kan de private sleutel gevonden worden en is het systeem gebroken. De veiligheid van RSA is dus gebaseerd op het getal factorisatie probleem, dat ‘moeilijk’ is. De lengte van de RSA sleutel is de lengte in bits van de modulus.

Vergelijkbaar met de moeilijkheid van het getal factorisatie probleem is het zogenaamde discrete logaritme probleem in bepaalde "groepen". Hierop kunnen cryptosytemen gebaseerd worden, dit valt buiten de scope van dit artikel. Belangrijk voor de veiligheid van zulke systemen is:

- de structuur van de groep;
- de grootte van de groep, d.w.z. het aantal elementen in de groep.

Bij een TDL systeem, is de structuur van de groep (en het cryptografische systeem) gebaseerd op "modulo een basis priemgetal p rekenen". De grootte van de groep is gelijk aan p-1. Met de lengte van een TDL sleutel wordt de lengte in bits van het basis priemgetal p bedoeld. Voorbeelden van TDL systemen zijn ElGamal (Elg) en Diffie-Hellman (DH) systemen, beiden worden ondersteund in Pretty Good Privacy.

Wassenaar Arrangement. Binnen het Wassenaar Arrangement is de maximale sleutel lengte voor RSA en TDL systemen gesteld op 512 bits, d.w.z., bovengenoemde RSA modulus en basis priemgetal p moeten kleiner zijn dan 2^{512}. Een populaire keuze voor beide lengten is 1024 bits.

Subgroep discrete logaritme systemen

Subgroep discrete logaritme (SDL) systemen lijken erg op traditionele discrete logaritme systemen, zij gebruiken dezelfde structuur voor de constructie van de groep met behulp van een basis priemgetal p. Zij gebruiken daarentegen slechts een gedeelte van de groep, een subgroep. De grootte van de subgroep, aangegeven met q, is een priemgetal dat p-1 deelt. Aanvallen op TDL systemen zijn ook van toepassing op SDL systemen. Er zijn echter ook aanvallen op SDL systemen die met name werken indien het groep priemgetal q relatief klein is. Onder de sleutellengtes bij een SDL systeem worden de lengte in bits van het basis priemgetal p en het groep priemgetal q bedoeld.

Wassenaar Arrangement. Binnen het Wassenaar Arrangement zijn geen maximale SDL sleutel lengten gesteld voor het groep priemgetal q, alleen voor de maximale lengte van het basis priemgetal p. Deze is vastgesteld op 512 bits. Een populaire sleutellengte is 160 bits voor het groep priemgetal q. Deze lengte wordt onder andere gebruikt in de US Digital Signature Algorithm, waarbij de lengte van het basis priemgetal p varieert tussen de 512 en 1024 bits.

Elliptische kromme systemen

Bij elliptische kromme (EK) discrete logaritme systemen is de groepstructuur gebaseerd "op de punten op een Elliptische Kromme" (denk aan een kromme in het vlak). De grootte van de groep q is wederom een priemgetal en de lengte van het groep priemgetal q geeft de EK sleutellengte.

Wassenaar Arrangement. Binnen het Wassenaar Arrangement is de maximale EK sleutel lengte gesteld op 112 bits. Een populaire keuze voor de EK sleutel lengte is 160 bits.