Selecting Cryptographic Key Sizes

Zusammenfassung des Artikels von Arjen K. Lenstra and Eric R. Verheul

Fabian Steiner
fabian.steiner@mytum.de

Sommerakademie der Studienstiftung des Deutschen Volkes,
Arbeitsgruppe „Applied Cryptography and Security Engineering“

Warum spielt die Länge von kryptographischen Schlüsseln eine Rolle?

- in vielen Bereichen des alltäglichen Lebens müssen Informationen verschlüsselt übertragen werden
  - Übermittelung der Bankdaten während eines Bestellvorgangs bei Ebay oder Amazon
  - Versenden von verschlüsselten Mails

Warum spielt die Länge von kryptographischen Schlüsseln eine Rolle?

- in vielen Bereichen des alltäglichen Lebens müssen Informationen verschlüsselt übertragen werden
  - Übermittelung der Bankdaten während eines Bestellvorgangs bei Ebay oder Amazon
  - Versenden von verschlüsselten Mails
- dennoch soll das Ganze so schnell wie möglich ohne größere Verzögerungen ablaufen
  - Notwendigkeit schneller kryptographischer Algorithmen
  - zu große Schlüssellängen sollten daher vermieden werden

Warum spielt die Länge von kryptographischen Schlüsseln eine Rolle?

- in vielen Bereichen des alltäglichen Lebens müssen Informationen verschlüsselt übertragen werden
  - Übermittelung der Bankdaten während eines Bestellvorgangs bei Ebay oder Amazon
  - Versenden von verschlüsselten Mails
- dennoch soll das Ganze so schnell wie möglich ohne größere Verzögerungen ablaufen
  - Notwendigkeit schneller kryptographischer Algorithmen
  - zu große Schlüssellängen sollten daher vermieden werden
- ABER: je kleiner die Länge eines Schlüssels, umso leichter ist dieser auch zu „knacken“

Symmetrische Kryptosysteme

- Personen S (Sender) und E (Empfänger) teilen sich einen geheimen Schlüssel, der sowohl für die Ver- als auch zur Entschlüsselung genutzt wird und daher geheim gehalten werden muss
- Verteilung des Schlüssels an S und E, bevor überhaupt eine Verschlüsselung stattfinden kann

Example

- DES (data encryption standard): entwickelt von IBM und NSA im Jahre 1977, 64 bit Schlüssellänge (56 bit effektiv zur Verschlüsselung, 8 bit Parity-Check)
- 2DES, 3DES: Nachfolger von DES mit 112 bzw. 168 bit Schlüssellänge
- AES (advanced encryption standard): aktueller „Stand der Technik“, Schlüssellängen von 128, 192 und 256 bit

Symmetrische Kryptosysteme, Fortf.

Angriffe

- trotz jahrzehntelanger Forschung keine bessere Methode bekannt, als einfach alle Schlüssel durchzuprobieren
- im Falle von DES müssten $2^{56} \approx 7.2 \cdot 10^{16}$ Schlüssel durchprobiert werden - dies stellt heutzutage kein Problem mehr dar
- Lenstra und Verheul erwarten in diesem Bereich keinerlei größere Fortschritte
- stattdessen: sollte sich ein symmetrisches Kryptosystem tatsächlich schneller entschlüsseln lassen, wird dieses nicht mehr verwendet werden

Asymmetrische Kryptosysteme

- E besitzt einen privaten Schlüssel und einen dazu passenden öffentlichen Schlüssel, der jedem (einschließlich dem Sender S) zugänglich gemacht werden darf
- Verschlüsselung erfolgt mit dem öffentlichen Schlüssel
- Entschlüsselung nur durch E mit Hilfe des privaten Schlüssels möglich
- wenn der private Schlüssel aus dem öffentlichen Schlüssel heraus berechnet werden kann, gilt ein solches System als gebrochen

Example

- klassische asymetrische Systeme (RSA [Rivest, Shamir, Adleman], TDL [Traditional Discrete Logarithm])
- subgroup discrete logarithm systems (SDL)
- elliptische Kurven (EC)

Assymmetrische Kryptosysteme, Fortf.

Angriffe

- RSA, TDL: Sicherheit beruht auf der Problematik, große Zahlen in ihre Primteiler zu zerlegen bzw. ihren diskreten Logarithmus zu berechnen
  - n bit RSA Schlüssel: Testen aller Primzahlen bis $\sqrt{n}$
  - Restklassenkörper $\mathbb{Z}_p$ (p Primzahl): bis zu p Rechenvorgänge notwendig
  - ABER: es sind bessere Methoden bekannt, z.B. Number Field Sieve (NFS)
  - $\Rightarrow$ Effizienz derartiger Verfahren verbessert sich fortlaufend
- SDL, EC: angreifbar durch ein von John M. Pollard entwickeltes Verfahren
  - seit damals keine weiteren Verbesserungen
  - entsprechendes wird daher auch von Lenstra und Verheul für die Zukunft angenommen

Kryptographische Hash-Funktionen

- Funktionen, die eine Nachricht beliebiger Länge in einen Hash fester Länge umwandelt
- kollisionsresistent: ($H(x)$ sei eine Hash-Funktion: $s, t \in \Sigma = \{0,1\}^*, s \neq t \wedge H(s) \neq H(t)$); impliziert pre-image und second-pre-image resistance
- Einwegfunktion: ($H^{-1}(x)$ darf nur äußerst schwer oder überhaupt nicht berechenbar sein)

Example

- MD4
- MD5
- SHA-1, SHA-2
- RIPEMD-160

Kryptographische Hash-Funktionen, Fortf.

Angriffe

- Angriff erfolgt mit Hilfe des sog. „Geburtstags Paradoxon“
- in einer Gruppe aus mind. 23 Leuten ist die Wahrscheinlichkeit, dass zwei Personen am gleichen Tag Geburtstag haben, größer als 50%
- die weiterführenden Bemerkungen für symmetrische Kryptosysteme gelten auch hier

Schlüsselpunkte

- Zeitspanne: wie lange soll der Schlüssel benutzt werden?

Schlüsselpunkte

- Zeitspanne: wie lange soll der Schlüssel benutzt werden?
- Sicherheitsrahmen: erwünschtes bzw. erhofftes Maß an Sicherheit (x)

Schlüsselpunkte

- Zeitspanne: wie lange soll der Schlüssel benutzt werden?
- Sicherheitsrahmen: erwünschtes bzw. erhofftes Maß an Sicherheit (x)
- Rechenleistung: erwartete Zunahme der verfügbaren Rechenleistung (x)

Schlüsselpunkte

- Zeitspanne: wie lange soll der Schlüssel benutzt werden?
- Sicherheitsrahmen: erwünschtes bzw. erhofftes Maß an Sicherheit (x)
- Rechenleistung: erwartete Zunahme der verfügbaren Rechenleistung (x)
- Kryptoanalytik: erwartete Fortschritte in der Krytoanalytik (x)

Sicherheitsrahmen

"sufficiently infeasible"

- Ausdruck schwierig mathematisch richtig zu beschreiben
- man ist versucht, relative Vergleiche anzustellen: „neuer Schlüssel muss 10^6 mal schwieriger zu berechnen sein als der Alte"

Lenstra und Verheul schlagen einen anderen Ansatz vor:

Sicherheitsrahmen, Fortf.

Definition

Der Sicherheitsrahmen s sei das Jahr, bis zu dem man das DES-Verfahren als sicher erachtet hat.

Annahme: $\boxed{s = 1982}$

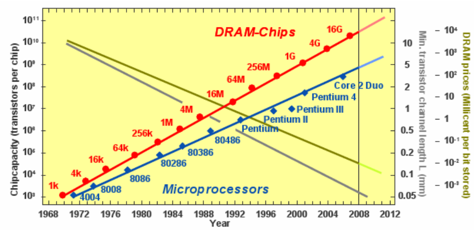
Hintergrund: aufgrund der großen Verbreitung und langen Einsatzdauer können sich viele Benutzer etwas unter dieser Definition vorstellen; die Wahl von $s = 1982$ begründet sich damit, dass DES 1977 erfunden wurde und seine Sicherheit alle fünf Jahre neu bewertet werden sollte

Rechenleistung

Definition

Die Variable $m > 0$ sei die Anzahl der Monate, nach denen mit einer Verdopplung der Prozessor-Geschwindigkeit zu rechnen ist.
Annahme: $\boxed{m = 18}$

Hintergrund: gemäß des Moore'schen Gesetzes ist alle 18 Monate eine Verdopplung der Rechenleistung zu erwarten



ITRS roadmap 99, 07

Definition

Die Variable $t \in \{0, 1\}$ legt fest, wie das vorhergehende m verstanden werden muss.

- $t = 1$: Rechenleistung und Speicher, die man für einen Doller erhält, verdoppelt sich alle m Monate
- $t = 0$: Rechenleistung und Speicher verdoppeln sich - ungeachtet des Preises - alle m Monate

Annahme $\boxed{t = 1}$

Hintergrund: grundsätzliche Annahme von $t = 0$ würde ein unendlich großes Budget von Organisationen implizieren, was kaum der Realität entsprechen kann

Definition

Die Variable $b > 0$ bestimmt die Anzahl der Jahre, nach denen eine Budget-Verdoppelung aufgrund allgemeiner wirtschaftlicher Weiterentwicklungen für eine Organisation zu erwarten ist.

Annahme: $\boxed{b = 10}$

Hintergrund: Statistiken auf der Grundlage des Bruttoinlandprodukts (BIP) der USA zeigen, dass obige Annahme gerechtfertigt ist

Kryptoanalytik

Definition

Die Variable $r > 0$ entspricht der Anzahl der Monate, nach denen sich kryptoanalytische Methoden für asymmetrische Systeme in ihrer Effizienz verdoppeln.

Annahme: $\boxed{\mathrm{r} = 18}$

Hintergrund: obige Annahme basiert auf den Forschungserfahrungen der vergangenen 25 Jahren

Bemerkungen

- nachdem obige Variablen s, m, t, b und r sowie drei weitere sinnvoll miteinader in Beziehung gesetzt werden, ergeben sich mehrere Formeln, die zu einer Berechnungsmöglichkeit für zukünftig realistische Schlüssellängen führen
- die Ergebisse hiervon müssen als angenäherte untere Grenzen verstanden werden
- die Sicherheit basierend auf den sich ergebenden Schlüssellängen ist mindestens gleich der von DES im Jahre s
- Formeln gelten auch dann, wenn einige Parameter abgeändert werden
- für weitere, tiefgreifendere Informationen sei auf den Artikel verwiesen (S. 28-30)

Untere Grenze für Schlüssellängen

Table 1. Lower bounds for computationally equivalent key sizes, assuming $s = 1982$, $m = 18$, $t = 1$, $b = 10$, $r = 18$, $c = 0$ and $c = 18$, $v = 1$.

Year	Symmetric Key Size	Classical Asymmetric Key Size and SDL Field Size		SDL Key Size	Elliptic Curve Key Size $c = 0$	Elliptic Curve Key Size $c = 18$	Infeasible number of Mips-Years	Lower bound for hardware cost in US$ for a 1 day attack (cf. 4.5)	Corresponding number of years on a 450MHz Pentium II PC
1982	56	417	288	102	105	*85*	$5.00 * 10^5$	$3.98 * 10^7$	$1.11 * 10^3$
1984	58	463	320	105	108	*89*	$1.45 * 10^6$	$4.57 * 10^7$	$3.22 * 10^3$
1986	60	513	352	107	111	*96*	$4.19 * 10^6$	$5.25 * 10^7$	$9.31 * 10^3$
1988	61	566	384	109	114	*101*	$1.21 * 10^7$	$6.04 * 10^7$	$2.69 * 10^4$
1990	63	622	448	112	117	*106*	$3.51 * 10^7$	$6.93 * 10^7$	$7.80 * 10^4$
1991	63	652	448	113	119	*109*	$5.97 * 10^7$	$7.43 * 10^7$	$1.33 * 10^5$
1992	64	682	480	114	120	*112*	$1.02 * 10^8$	$7.96 * 10^7$	$2.26 * 10^5$
1993	65	713	512	116	121	*114*	$1.73 * 10^8$	$8.54 * 10^7$	$3.84 * 10^5$
1994	66	744	544	117	123	*117*	$2.94 * 10^8$	$9.15 * 10^7$	$6.53 * 10^5$
1995	66	777	544	118	124	*121*	$5.00 * 10^8$	$9.81 * 10^7$	$1.11 * 10^6$
1996	67	810	576	120	126	*122*	$8.51 * 10^8$	$1.05 * 10^8$	$1.89 * 10^6$
1997	68	844	608	121	127	*125*	$1.45 * 10^9$	$1.13 * 10^8$	$3.22 * 10^6$
1998	69	879	640	122	129	*129*	$2.46 * 10^9$	$1.21 * 10^8$	$5.48 * 10^6$
1999	70	915	672	123	130	130	$4.19 * 10^9$	$1.29 * 10^8$	$9.31 * 10^6$
2000	70	952	704	125	132	132	$7.13 * 10^9$	$1.39 * 10^8$	$1.58 * 10^7$
2001	71	990	736	126	133	135	$1.21 * 10^{10}$	$1.49 * 10^8$	$2.70 * 10^7$
2002	72	1028	768	127	135	139	$2.06 * 10^{10}$	$1.59 * 10^8$	$4.59 * 10^7$
2003	73	1068	800	129	136	140	$3.51 * 10^{10}$	$1.71 * 10^8$	$7.80 * 10^7$
2004	73	1108	832	130	138	143	$5.98 * 10^{10}$	$1.83 * 10^8$	$1.33 * 10^8$
2005	74	1149	864	131	139	147	$1.02 * 10^{11}$	$1.96 * 10^8$	$2.26 * 10^8$
2006	75	1191	896	133	141	148	$1.73 * 10^{11}$	$2.10 * 10^8$	$3.84 * 10^8$
2007	76	1235	928	134	142	152	$2.94 * 10^{11}$	$2.25 * 10^8$	$6.54 * 10^8$
2008	76	1279	960	135	144	155	$5.01 * 10^{11}$	$2.41 * 10^8$	$1.11 * 10^9$
2009	77	1323	1024	137	145	157	$8.52 * 10^{11}$	$2.59 * 10^8$	$1.89 * 10^9$

(s.a. A. Lenstra, E. Verheul: "Selecting Cryptographic Key Sizes", S. 32)

Untere Grenze für Schlüssellängen, Fortf.

2010	78	1369	1056	138	146	160	$1.45 * 10^{12}$	$2.77 * 10^{8}$	$3.22 * 10^{9}$
2011	79	1416	1088	139	148	163	$2.47 * 10^{12}$	$2.97 * 10^{8}$	$5.48 * 10^{9}$
2012	80	1464	1120	141	149	165	$4.19 * 10^{12}$	$3.19 * 10^{8}$	$9.32 * 10^{9}$
2013	80	1513	1184	142	151	168	$7.14 * 10^{12}$	$3.41 * 10^{8}$	$1.59 * 10^{10}$
2014	81	1562	1216	143	152	172	$1.21 * 10^{13}$	$3.66 * 10^{8}$	$2.70 * 10^{10}$
2015	82	1613	1248	145	154	173	$2.07 * 10^{13}$	$3.92 * 10^{8}$	$4.59 * 10^{10}$
2016	83	1664	1312	146	155	177	$3.51 * 10^{13}$	$4.20 * 10^{8}$	$7.81 * 10^{10}$
2017	83	1717	1344	147	157	180	$5.98 * 10^{13}$	$4.51 * 10^{8}$	$1.33 * 10^{11}$
2018	84	1771	1376	149	158	181	$1.02 * 10^{14}$	$4.83 * 10^{8}$	$2.26 * 10^{11}$
2019	85	1825	1440	150	160	185	$1.73 * 10^{14}$	$5.18 * 10^{8}$	$3.85 * 10^{11}$
2020	86	1881	1472	151	161	188	$2.94 * 10^{14}$	$5.55 * 10^{8}$	$6.54 * 10^{11}$
2021	86	1937	1536	153	163	190	$5.01 * 10^{14}$	$5.94 * 10^{8}$	$1.11 * 10^{12}$
2022	87	1995	1568	154	164	193	$8.52 * 10^{14}$	$6.37 * 10^{8}$	$1.89 * 10^{12}$
2023	88	2054	1632	156	166	197	$1.45 * 10^{15}$	$6.83 * 10^{8}$	$3.22 * 10^{12}$
2024	89	2113	1696	157	167	198	$2.47 * 10^{15}$	$7.32 * 10^{8}$	$5.48 * 10^{12}$
2025	89	2174	1728	158	169	202	$4.20 * 10^{15}$	$7.84 * 10^{8}$	$9.33 * 10^{12}$
2026	90	2236	1792	160	170	205	$7.14 * 10^{15}$	$8.41 * 10^{8}$	$1.59 * 10^{13}$
2027	91	2299	1856	161	172	207	$1.21 * 10^{16}$	$9.01 * 10^{8}$	$2.70 * 10^{13}$
2028	92	2362	1888	162	173	210	$2.07 * 10^{16}$	$9.66 * 10^{8}$	$4.59 * 10^{13}$
2029	93	2427	1952	164	175	213	$3.52 * 10^{16}$	$1.04 * 10^{9}$	$7.81 * 10^{13}$
2030	93	2493	2016	165	176	215	$5.98 * 10^{16}$	$1.11 * 10^{9}$	$1.33 * 10^{14}$
2032	95	2629	2144	168	179	222	$1.73 * 10^{17}$	$1.27 * 10^{9}$	$3.85 * 10^{14}$
2034	96	2768	2272	171	182	227	$5.01 * 10^{17}$	$1.46 * 10^{9}$	$1.11 * 10^{15}$
2036	98	2912	2400	173	185	232	$1.45 * 10^{18}$	$1.68 * 10^{9}$	$3.22 * 10^{15}$
2038	99	3061	2528	176	188	239	$4.20 * 10^{18}$	$1.93 * 10^{9}$	$9.33 * 10^{15}$
2040	101	3214	2656	179	191	244	$1.22 * 10^{19}$	$2.22 * 10^{9}$	$2.70 * 10^{16}$
2042	*103*	*3371*	*2784*	*182*	*194*	*248*	$3.52 * 10^{19}$	$2.55 * 10^{9}$	$7.82 * 10^{16}$
2044	*104*	*3533*	*2944*	*185*	*197*	*255*	$1.02 * 10^{20}$	$2.93 * 10^{9}$	$2.26 * 10^{17}$
2046	*106*	*3700*	*3072*	*187*	*200*	*260*	$2.95 * 10^{20}$	$3.36 * 10^{9}$	$6.55 * 10^{17}$
2048	*107*	*3871*	*3232*	*190*	*203*	*265*	$8.53 * 10^{20}$	$3.86 * 10^{9}$	$1.90 * 10^{18}$
2050	*109*	*4047*	*3392*	*193*	*206*	*272*	$2.47 * 10^{21}$	$4.44 * 10^{9}$	$5.49 * 10^{18}$

(s.a. A. Lenstra, E. Verheul: "Selecting Cryptographic Key Sizes", S. 32)

Weiterführende Literatur

- Arjen K. Lenstra, Eric R. Verheul. Selecting cryptographic key sizes. Journal of Cryptology, 14(4):255–293, 2001.
- `http://www.keylength.com/` - Online Berechnung von sinnvollen Schlüssellängen anhand verschiedener Modelle und Parameter