1024 bit RSA

ist nicht mehr sicher!

Ruediger Weis

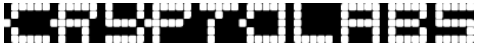
cryptolabs Amsterdam

Aktuelle Übersichtsartikel

Ruediger Weis & Andreas Bogk & Stefan Lucks

- ”1024 bit reichen wohl nicht mehr”,
  CCC Datenschleuder, 2003.
- ”Sicherheit von 1024 bit RSA Schlüsseln gefährdet”,
  Datenschutz und Datesicherheit (DuD), 2003.

`http://www.cryptolabs.org/rsa/`



Vor 4 Jahren

CCCongress 1999

- Hauptspeicher < 3 GB für 512-bit Modulus.

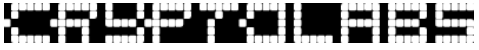
RSA

Ron Rivest, Adi Shamir, Leonard Adleman

- A method for obtaining digital signatures and public-key cryptosystems,

Communications of the ACM, 21(2),

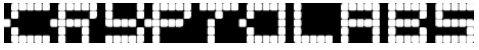
Februar 1978.



23.01.2003

Adi Shamir, Eran Tromer

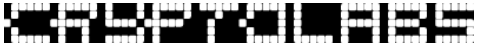
- Primaly Draft



Kostenabschätzungen

- 512 bit Keys: 10.000 € Hardware
  $\rightarrow$ 10 min
- 1024 bit Keys: 10.000.000 € Hardware
  $\rightarrow$ 1 Jahr

in der Theorie ...



Sieb-Algorithmen

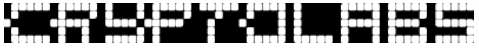
- Siebungsschritt
- Gleichungssystem Schritt

Komplexität GNFS

$$\mathcal{O}\left(exp\left[(1,92+\mathcal{O}(1))*(\ln(n))^{1/3}*(\ln(\ln(n)))^{2/3}\right]\right)$$

Siebungsschritt

- Zahlen suchen mit bestimmter Eigenschaft (Smoothness)
- Hochgradig parallelisierbar

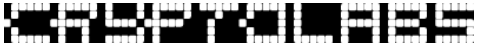


Mathmatische Details I

Eine Instanz eines "Sieb-Problems" besteht aus einer ganzen Zahl R, einem Schwellwert T und Paaren (r_i, p_i), wobei p_i eine kleine Primzahl ist.

Die Paare (r_i, p_i) definieren ”Progressionen”

$$P_i = \{a | a \text{ mod } p_i = r_i\}.$$



Mathmatische Details II

Beim "Sieb-Problem" geht es darum, möglichst viele Werte a zu finden, mit

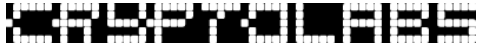
$$\sum_{i:a \in P_i} \log(p_i) > T.$$

Spezialhardware

Grob vereinfacht kann man Geräte wie TWIRL als Spezialhardware auffassen, die dazu dient, die Summen

$$\sum_{i:a \in P_i} \log(p_i)$$

mit Einsatz von möglichst wenig Chipfläche zu berechnen.



Matrixreduktion

- Weis, R., CCC 1999: 'Home PC'
- Lenstra, Shamir, Tomlinson, Tromer, "Analysis of Bernstein's Factorization Circuit" ASIACRYPT 2002

  "... the security of RSA relies exclusively on the hardness of the relation collection step of the number field sieve."

D.J. Bernstein

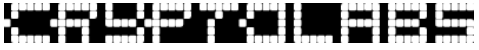
- Neuartigen Ansatz zur effizienten Implemenation der Matrix-Reduktion
- Neues Kostemass
- ’Lange Zahlen’

Mathematische Trivialitäten

- Parallelisierbarkeit
- Wiedernutzbarkeit

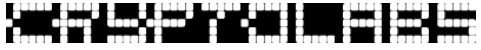
Parallelisierbarkeit

- Das Verfarhen ist nahezu beliebig parallelisierbar.
- Beispielsweise mit Hardware für 120 Millionen Euro
  $\rightarrow$ 1 Monat.
- Rest Übungsaufgabe ...



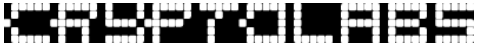
Wiedernutzbarkeit

- Hardware kann für mehrere Schlüssel (nacheinander) verwendet werden.



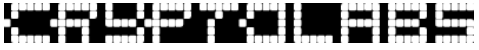
Weizmann Institute

- TWINKLE: Gallium-Arsenid-Technologie
- TWIRL: Silizum-Technologie



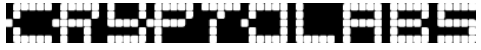
Hardware Analyse TWINKLE

- Gallium-Arsenid-Technologie
- 512-Bit-Keys Wafer mit 30cm Durchmesser



Hardware Analyse TWIRL

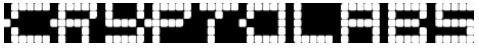
- Silizium-basierter VLSI-Technologie
- 0.13μ Strukturgrösse
- $1423\ mm^2$ pro Chip für 1024 Bit Modulus



TCG keys MUST be 2048 bit RSA or greater

TCG1.2 (Part 1, P.12 f.)

- ”All Storage keys MUST be of strength equivalent to a 2048 bit RSA key or greater.”
- ”The minimum RECOMENDED key size is 2048 bits.”



Cryptophone: 4096 bit

DH 4096 bit (DLP basiert)

- Selbst auf aktuellen PDAs sind 4096 bit Public Key-Verfahren Verfahren machbar.

`http://www.cryptophone.de/`

”Produkt!”

Acknowledgments

- Stefan Lucks, Andreas Bogk
- ©cryptolabs Amsterdam 2003
  under the GNU Free Document License.
- Produced with Free Software under
  GNU/Linux.