Einführung zu RSA

Andreas Zweili, Ismail Cadaroski, Ivan Hörler, Michael Stratighiou

28. Dezember 2016

Inhaltsverzeichnis

1 Einführung

Diese Arbeit wird eine Einführung zu dem Verschlüsselungsalgorithmus RSA geben. Anhand von vereinfachten Rechnungen wird die Funktion des Algorthmus veranschaulicht und erklärt. In der Realität sind die verwendeten Zahlen jedoch um ein x-faches grösser. Die nachfolgende Zahl ist 1024 Bit gross. Der Leser kann sich also ungefähr vorstellen wie gross die Zahlen sind wenn die heutige empfohlene Grösse bei 4096 Bit liegt.

RSA-1024 Primzahl

```
135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563
```

1.1 Geschichte

Im Jahre 1976 wurde von Whitfield Diffie und Martin Hellman eine Theorie zu Publickey-Kryptographie veröffentlicht. In welcher sie ein Konzept Namens FF-alltürpräsentieren. Dabei handelt es sich um mathematische Probleme welche in eine Richtung sehr aufwändig und in die andere Richtung viel einfacher zu lösen sind.

Ronald L. Rivest, Adi Shamir und Leonard Adleman wollten nach der Veröffentlichung der Theorie von Herrn Diffie und Herrn Hellman beweisen das solche Falltüren nicht existieren. Dabei entdeckten sie jedoch genau solch eine Falltür daraus entwickelten sie dann den RSA Algorithmus welchen sie 1977 vorstellten. RSA steht dabei für die Anfangsbuchstaben ihrer Familiennamen.

Im Jahre 2002 erhielten sie den Turing-Award für ihre Arbeit auf dem Gebiet der Kryptographie. Welcher oft als Nobel Preis für Informatik bezeichnet wird.

1.2 Verwendung

RSA wird heute in eine Vielzahl an Programmen eingesetzt. Von besonderer Wichtigkeit sind hier folgende Systeme zu Erwähnen.

Bankkarten nach dem EMV Standard

Dieser Standard definiert wie der Chip auf den Karten zu funktionieren hat und wie die Authentifizierung gegenüber den Bankautomaten funktioniert.

HTTPS (TLS und X.509-Zertifikate)

HTTPS garantiert das die Zugriffe auf Website welche es unterstützen, vor Manipulationen sowie Spionage von Unbefugten geschützt sind. Dies ist insbesondere bei eBanking oder Websiten mit Logins essentiel wichtig. Ansonsten ist es ein Leichtes Konten zu übernehmen.

SSH (Secure Shell)

SSH ist ein Protokoll mit welchem man remote auf Unix Systeme Zugreifen kann. Am häufigsten wird es genutzt zur Administrierung von Servern oder zur Übertragung von Dateien.

OpenPGP

OpenPGP ist ein Verschlüsselungsverfahren welches hauptsächlich bei der Verschlüsselung von Emails verwendet wird. Abseits davon wird es auch zur Signierung von Dateien eingesetzt.

Insgesamt

2 Verschlüsseln

TODO: Sind das wirklich alles Sections? Ich habe sie jetzt mal in Subsections geändert. Ist evtl. eher Fett gemeint? Ismail was hast du hier gemeint?

2.1 Schlüsselkontruktion

N = Privatschlüssel p= primzahl q = primzahl

Gleichung erstellen nach :

$$\begin{aligned}\varphi(N) &= \varphi(p * q)\\ &= \varphi(p) * \varphi(q)\\ &= (p-1) * (q-1)\end{aligned}$$

2.2 Wählen der Variablen

$$\begin{aligned}p &= 7\\ q &= 11\\ \varphi(N) &= \varphi(11 * 7)\end{aligned}$$

2.3 Privatschlüssel

2.4 Öffentlicher Schlüssel

3 Verschlüsselung

Hallo Dies ist ein Test

4 Verteilung/Übertragung

Hallo Dies ist ein Test

5 Entschlüsselung

Hallo Dies ist ein Test

6 Schwachstellen

Hallo Dies ist ein Test

7 Referenzen

Literatur

[1] L. Van Houtven. Crypto 101, 2016. https://www.crypto101.io.

[2] R.L. Rivest und A. Shamir und L. Adleman. A method for obtaining digital signatures and public-key cryptosystems, 1978. https://people.csail.mit.edu/rivest/Rsapaper.pdf.

[3] Whitfield Diffie und Martin Hellman. New directions in cryptographie, 1976. https://www-ee.stanford.edu/%7Ehellman/publications/24.pdf.

[4] Wikipedia. Diffie-Hellman-Schlüsselaustausch — Wikipedia, Die freie Enzyklopädie, 2016. https://de.wikipedia.org/wiki/Diffie-Hellman-Schl%C3%BCsselaustausch.

[5] Wikipedia. Hybride Verschlüsselung — Wikipedia, Die freie Enzyklopädie, 2016. https://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsselung.

[6] Wikipedia. RSA (cryptosystem) — Wikipedia, Die freie Enzyklopädie, 2016. https://en.wikipedia.org/wiki/RSA_(cryptosystem).

[7] Wikipedia. RSA-Kryptosystem — Wikipedia, Die freie Enzyklopädie, 2016. https://de.wikipedia.org/wiki/RSA-Kryptosystem.