

Bernd Borchert

Univ. Tübingen WS 13/14

Vorlesung

Kryptographie

Teil 6

6.12.13

Asymmetrische Verschlüsselungsverfahren

- RSA (Kurz wiederholung)
- Rabin
- Elgamal
- Elliptische Kurven (nicht heute)

RSA Kryptoverfahren

- 1977
- beruht auf Faktorisierungsproblem
- immer noch das Standard Public-Key Verfahren, wobei heutzutage auch oft Elgamal oder Elliptische Kurven genommen werden.
- bis ca. 850 bit durch Supercomputer brechbar. RSA1024 ist somit noch sicher, aber besser ist RSA2048.

RSA Schlüsselpaar-Erzeugung

Wähle zufällig zwei Primzahlen p und q , die ungefähr lang sind. Sei $N = pq$. Berechne $\phi(N)$ (Euler Funktion)

Wähle eine zu $\phi(N)$ teilerfremde Zahl $e < \phi(N)$.

Berechne d , für das gilt: $ed = 1 \bmod \phi(N)$ (via erweiterter Euklid)

(e, N) ist öffentlicher Schlüssel, (d, N) der private.

RSA
Public Key
(e, N)

RSA
Private Key
(d, N)

RSA Verschlüsselung

Ein m aus $\{0, \dots, N-1\}$ wird mit dem öffentlichen Schlüssel verschlüsselt zu

$$c = m^e \bmod N$$

RSA
Public Key
(e, N)

RSA
Private Key
(d, N)

RSA Entschlüsselung

Ein Ciphertext c aus $\{0, \dots, N-1\}$ wird mit dem privaten Schlüssel entschlüsselt zu

$$c^d \bmod N$$

Verifikation: $c^d = m^{\text{ed}} = m^{1 - Y \text{ phi}(N)} = m \bmod N$
(Euler/Fermat)

RSA
Public Key
(e, N)

RSA
Private Key
(d, N)

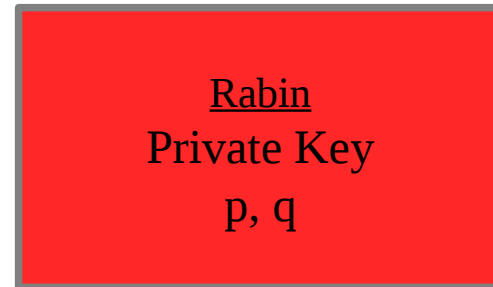
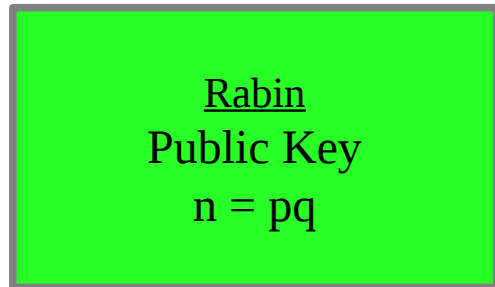
Rabin Kryptoverfahren

- 1979
- Verwandt mit RSA
- Idee: im Modulo-Ring eines Primzahlprodukts quadrieren, statt wie bei RSA potenzieren
- Nachteil: es ist keine Bijektion, sondern jeder Kryptotext hat 4 Plaintexts
- Sicherheit äquivalent zum Faktorisierungsproblem
- In der Praxis nicht relevant

Rabin Schlüsselpaar-Erzeugung

Wähle zufällig 2 große Primzahlen p und q , die beide 3 modulo 4 sind.

Der öffentliche Schlüssel besteht aus dem Produkt $n = pq$,
der private aus p und q .



Rabin Verschlüsselung

Ein m aus $\{0, \dots, n-1\}$ wird mit dem öffentlichen Schlüssel verschlüsselt zu

$$c = m^2 \bmod n$$

Rabin
Public Key
 $n = pq$

Rabin
Private Key
 p, q

Rabin Entschlüsselung

Ein c aus $\{0, \dots, n-1\}$ wird mit dem Schlüssel entschlüsselt zu den 4 Lösungen

$$r = (vpe + wqf) \bmod n$$

$$r' = n - r$$

$$s = (vpe - wqf) \bmod n$$

$$s' = n - s$$

v, w def. als Mult. Inverse von p modulo q
bzw. q modulo p (CRT mit 2 Gleichungen)
 $e := c^{(q+1)/4} \bmod q$
 $f := c^{(p+1)/4} \bmod p$
(wg. Euler Kriterium gilt
 $e^2 = c \bmod p, f^2 = c \bmod q$)

Welche Lösung die richtige ist, muss geraten werden.

Rabin
Public Key
 $n = pq$

Rabin
Private Key
 p, q

Euler Kriterium

$$\begin{aligned} c^{(p-1)/2} &= 1 \bmod p \text{ wenn es ein } b \text{ gibt mit } b^2 = c \bmod p \\ &= -1 \bmod p \text{ sonst} \end{aligned}$$

Anwendung auf Verifikation Rabin Kryptosystem:

Vorbem. Weil $p \bmod 3$ ist (Vorgabe), ist in $e = c^{(p+1)/4}$ der Exponent eine Ganzzahl, ebenso f .

Weil $c = m^2 \bmod pq$ (Verschlüsselungsaktion) ist auch $c = m^2 \bmod p$.

Also ist wg. Euler Kriterium:

$$e^2 = (c^{(p+1)/4})^2 = c^{(p+1)/2} = c c^{(p-1)/2} = c \bmod p.$$

Ebenso ist $f^2 = c \bmod q$.

Elgamal Kryptoverfahren

- 1985
- beruht auf Diskreter Logarithmus (DL):

Gegeben Primzahl p , a und m aus $\{0, \dots, p-1\}$.
Für welches x aus $\{0, \dots, p-1\}$ gilt $a^x = m \bmod p$?

- Sicherheit äquivalent zum DL Problem

Elgamal Schlüsselpaar-Erzeugung

Wähle q , so dass q und $p = 2q + 1$ beides Primzahlen sind.

Wähle g aus $\{q+1, \dots, p-2\}$ und ein zufälliges a aus $\{2, \dots, p-1\}$ und berechne $A := g^a \bmod p$.

Der öffentliche Schlüssel ist (p, g, A) , der private ist a .

Elgamal
Public Key
 (p, g, A)

Elgamal
Private Key
 a

Elgamal Verschlüsselung

Ein m aus $\{0, \dots, p-1\}$ wird mit dem öffentlichen Schlüssel zu einem Ciphertext (B, c) verschlüsselt:

Wähle zufälliges b aus $\{0, \dots, p-1\}$.

Sei $B := g^b \bmod p$ und $c := A^b m \bmod p$

Der Ciphertext ist das Paar (B, c) .

Elgamal
Public Key
 (p, g, A)

Elgamal
Private Key
 a

Elgamal Entschlüsselung

Ein Ciphertext (B,c) wird mit dem privaten Schlüssel entschlüsselt zu

$$B^{p-1-a} c \bmod p$$

Verifikation: $B^{p-1-a} c = g^{b(p-1-a)} A^b m = g^{b(p-1-a)} g^{ab} m =$

$$g^{b(p-1)} g^{-ab} g^{ab} m = g^{(p-1)b} m = m \bmod p \quad (\text{kleiner Fermat})$$

Elgamal
Public Key
(p,g,A)

Elgamal
Private Key
a

CRT mit n Gleichungen

Gegeben Gleichungssystem der Form

$$x = a_1 \bmod m_1$$

...

$$x = a_n \bmod m_n$$

mit $m_1, \dots, m_n$ gegenseitig teilerfremd.

Eine Lösung x_0 existiert und ist nicht nur modulo dem Produkt $m := m_1 \cdots m_n$ eindeutig bestimmt, sondern kann angegeben werden als
Summe

$$x_0 = a_1 M_1 e_1 + \dots + a_n M_n e_n$$

wobei $M_i = m/m_i$, und e_i das mult. Inverse von M_i modulo m_i ist.

Alle weiteren Lösungen ergeben sich als $x_0 + zm$ für Ganzzahlen z .

(Ursprung: Sun Zi, China, ca. 300 europ. Zeitrechnung)

CRT mit 2 Gleichungen

Gegeben Gleichungssystem der Form

$$x = a_1 \bmod m_1$$

$$x = a_2 \bmod m_2$$

mit m_1 und m_2 teilerfremd.

Seien r das mult. Inverse von m_2 modulo m_1 , und s das von m_1 modulo m_2 .

Dann ist $x = a_1 r m_2 + a_2 s m_1$ eine Lösung, und (alle) weiteren ergeben sich durch Aufaddieren von $z m_1 m_2$ für Ganzzahlen z .

Wiederholung

Multiplikatives Inverses

Beispiel.

Gesucht das multiplikative Inverse e von 9 modulo 23, also $9e = 1 \pmod{23}$.

Erweiterter Euklid:

$$23 = 2 \cdot 9 + 5$$

$$9 = 1 \cdot 5 + 4$$

$$5 = 1 \cdot 4 + 1$$

$$1 = 5 - 1 \cdot 4 = 5 - 1 \cdot (9 - 1 \cdot 5) = 2 \cdot 5 - 1 \cdot 9 = 2 \cdot (23 - 2 \cdot 9) - 1 \cdot 9 = 2 \cdot 23 - 5 \cdot 9$$

Also ist das Inverse e von 9 mod 23 gleich $-5 = 18 \pmod{23}$.

Test: $9 \cdot 18 = 162 = 7 \cdot 23 + 1$. Also ist $9 \cdot 18 = 1 \pmod{23}$.