

31.01.2006

Notiztitel

31.01.2006

Klausur

1 Blatt handgeschrieben
DIN A4.

2 Taschenrechner
kein Formelspeicher

$$p = 193 \neq \text{mod } 193$$

RSA Schlüsselzeugung
Verschlüsselung
Entschlüsselung
Optimierung mit CRT
Low exponent attack

Rabin analog

El Gamal Verschlüsselung

Schlüssel, Verschlüsselung, Entschlüsselung
generisch

Zusammenhang mit Diffie - Hellman (Problem)

El Gamal / DSA Signatur

Schlüssel, Signieren, Verifizieren

DSA \rightarrow Primitivwurzel

wie entscheidet man, ob g PW ist?

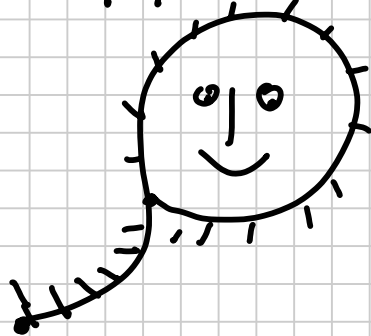
Wie berechnet man Element der Ordnung q ?
 Vergleich Effizienz RSA / DSA.

DL Shanks Babystep - Giantstep - Verfahren

$$m = \lceil \sqrt{|G|} \rceil, \quad g^x = a, \quad x = \underbrace{q \cdot m}_{\text{Giant}} + \underbrace{r}_{\text{Baby}}$$

Schranken für q, r ?

Pollard - Rho



Wann wird ein Match gefunden (bei der Spieluhr ist effizienteste Variante).

Berechnung DL

$$ax \equiv b \pmod{m}$$

wenn $\underbrace{\text{ggT}(a, m)}_{> 1} \mid b$

Index-Calculus

Wie berechnet man DL aus gegebenen Relationen?

Faktorisieren:

$(p-1)$ - Methode für ein kleines Beispiel

- Berechnung von k
- Bestimmung des Faktors $\text{ggT}(a^k - 1, n)$.

Quadratisches Sieb

$$(x+m)^2 - n$$

Nullstellen mod p ($p \leq n$)

x	1	3	5	7	9	11	13	15
$2 f(x)$								
$3 f(x)$		ja						
$5 f(x)$								
$7 f(x)$								
Rest		1				157		

↖
Relation

Relation \rightarrow Faktorisierung.

Hash funktionen

- (Auswirkung der) Geburtstagsparadoxie

$$h: \{0,1\}^* \rightarrow \{0,1\}^{120}$$

Endliche Körper

Konstruktion $F = \mathbb{F}_2[x] / p(x) | \mathbb{F}_2[x]$

Darstellung der Elemente

Addition, Multiplikation, Gesundheit,

$|F^*| = 2^n - 1$, zyklisch,

Nachweisen, dass Element ein Erzeuger ist

LA: Was ist die Matrix einer linearen Abb.? Wie findet man sie?

