Codierung CheatSheet

Verschlüsselungsverfahren

Perfekt sicherer Code

One-Time-pad code

- Codierungsschlüssel genau so lang wie der zu kodierende Text.
- Schlüssel zufällig
- Kommis sind nur aufgeflogen, weil sie die Schlüssel recycelt haben

Was bedeutet Perfekt?

$P(m) = P(m|C)$

Public-Key

Besteht aus öffentlichem und privaten Teil.
Der öffentliche ist wie ein offenes Schloss, der genutzt werden kann, um etwas nur mit dem privaten Schlüssel zugreifbar zu machen.

RSA

Basiert drauf das die Primzahlfaktorisierung NP-vollständig ist.

Erzeugung RSA-Code

- bestimme p,q die Primzahlen sind und weit genug auseinanderliegen
- dann $n = p * q$ und $\phi(n) = (p-1)(q-1)$:= #der Zahlen, die zu n teilerfremd sind.
- wähle öffentlichen Schlüssel e mit $ggt(\phi(n), e) = 1$
- finde durch EEA(erweiterter Euklidischen algorithmus) ein d sodass $e * d^{=}1(modphi(n))$
- mann verschlüsselt dann mit m^e und entschlüsselt mit $(m^e)^d$

Warum klappt codierung/decod.?

$ed = 1(modphi(n))$

Und wie genau?

$ed = 1 + k * phi(n)$
$m^(1 + k * phi(n))$
$m * m^(k * phi(n))$
$m * (m^(p-1))^(k * (q-1))$
$m * 1, daFermatsatz : m^(p-1) = 1(modp) - >= 1(modp * q)$

Wie funktioniert dann El-Gamal?

(p, g, g^a) öffentlich, a geheim
jemand wählt b (geheim) und sendet $(g^b, m * g^a b)$
Empfänger macht dann $(g^b a)^{-}1$ und kann so entschlüsseln

Warum sind die sicher, wenn $NP! = P$?

- RSA weil Primzahlzerlegung NP-vollständig
- El-Gamal weil es keinen diskreten Algo gibt

Und wenn $NP = P$...

Weltuntergang!
Bei NP kann man raten und dann in poly. berechnen, dauert halt ewig, weil man nur raten kann.
Wenn man jedoch nicht mehr raten muss, sondern z.B. Primfaktoren in poly. berechnen könnte, dann würde das Kartenhaus zusammenfallen.
Auf $NP! = P$ basiert unsere Sicherheit.

Was ist sicherer (RSA oder El Gamal)?

El Gamal, da sich der Schlüssel ändert.

Hat El Gamal auch Nachteile?

- **Hauptnachteil** ist, dass es sichere Zufallszahlen braucht
- Ausserdem wird der verschlüsselte Text doppelt so gross wie das Original (?)

Gegen was ist ElGamal immun, das RSA belastet?

Wörterbuchangriffe, da sich der Schlüssel bei RSA nicht ändert, kann er leichter erraten werden.

Welche Angriffe gibt es noch?

- known plaintext
- known chiffretext
- chosen plaintext
- chosen chiffretext
- man-in-the-middle