Kryptografie und -analyse, Zusammenfassung Vorlesung 9

Henry Haustein

Wie kann ein Generator einer Gruppe G gefunden werden?

Primfaktorzerlegung $|G| = p_1 \cdot p_2 \cdot ...$, Wahl eines zufälligen Elementes $a \in G$, für jedes p_i:

$$a^{\frac{|G\|}{p_i}} \stackrel{?}{\equiv} 1 \mod |G|$$

Wenn $\equiv 1$, dann a kein Generator.

Was versteht man unter dem Problem des Diskreten Logarithmus?

Bestimme x:

$$x = \log_g(y) \mod p$$

Wie funktioniert der BSGS-Algorithmus?

$m = \lceil \sqrt{|G|} \rceil$, Ansatz $x = qm + r$

- Babystep-Liste: $B = \{(i, y(g^i)^{-1}) \mod p\} \to r$
- Giantstep-Liste: $G = \{(j, (g^m)^j) \mod p\} \to q$

Berechnung der Elemente von G, bis $(g^m)^j$ als zweite Komponente eines Elements in B gefunden wurde.

Wie funktioniert der DH-Schlüsselaustausch?

Öffentlich: p, g, A wählt x_A, B wählt x_B, berechnet $y_A = g^{x_A} \mod p$, Austausch y_A, y_B, $\Rightarrow k = y_B^{x_A} \mod p$

Worauf beruht die Sicherheit (DH-Problem)?

Bestimme x_A (x_B analog):

$$x_A = \log_g(y_A) \mod p$$

Ist der DH-Schlüsselaustausch sicher gegen passive bzw. aktive Angriffe?

sicher gegen passive Angriffe, nicht sicher gegen aktive Angriffe (Man-in-the-middle)

Wie werden bei ElGamal die Schlüssel bestimmt?

Jeder Teilnehmer:

- wählt Primzahl p und Generator $p \in \mathbb{Z}_p^*$
- wählt zufällige Zahl k_d mit $0 \leq k_d \leq p-2$
- berechnet $k_e = g^{k_d} \mod p$

$\Rightarrow$ öffentlicher Schlüssel: (p, g, k_e)

$\Rightarrow$ privater Schlüssel: k_d

Wie funktioniert ElGamal als Konzelationssystem?

Verschlüsselung (B $\rightarrow$ A):

- B benötigt öffentlichen Schlüssel von A: (p, g, k_e)
- wählt Zufallszahl r mit $0 \leq r \leq p-2$
- berechnet: $c = (c_1, c_2)$ mit

$$c_1 = g^r \mod p$$
$$c_2 = mk_e^r \mod p$$

Entschlüsselung:

$$m = (c_1^{k_d})^{-1} c_2 \mod p$$

Worauf beruht die Sicherheit des ElGamal-Kryptosystems (DH-Problem, wie lautet es hier konkret)?

Bestimme k_d:

$$k_d = \log_g(k_e) \mod p$$

Was ist bei der sicheren Verwendung von ElGamal als Konzelationssystem zu beachten? (Warum darf die Zufallszahl nur einmal vewendet werden? Welcher aktive Angriff ist möglich? Wie ist er zu verhindern?)

Wenn die Zufallszahl mehrfach verwendet wird, so kann, falls eine Nachricht m_1 bekannt ist, eine andere Nachricht m_2 (bei selben r) berechnet werden.

Gewählter Klartext-Schlüsseltext-Angriff ist auch möglich $\Rightarrow$ Einfügen von Redundanz: $m = m, h(m)$