Inhalt

symmetrische vs asymmetrische Systeme

- **symmetrisches Krypto-System:**
  ”gleicher” Schlüssel für Verschlüsselung/Entschlüsselung
  (Bsp: One Time Pad, Cäsar-Verschlüsselung)

- **asymmetrisches Krypto-System:**
  verschiedene Schlüssel:
  e: **public key** (für Verschlüsselung)
  d: **private key** (für Entschlüsselung)
  (Bsp: RSA)

Public Key Verschlüsselung – Terminologie

Definition:

Ein **Public Key Krypto-System** besteht aus 3 (effizienten) Algorithmen:

1. **Schlüsselgenerator**: erzeugt Schlüsselpaar (e, d)
2. **Verschlüsselungs-Algorithmus**
3. **Entschlüsselungs-Algorithmus**

Anforderungen ans Krypto-System:

- **Entzifferbarkeit**
- **Sicherheit:** Ohne Kenntnis des geheimen Schlüssels ist es nicht möglich, die Nachricht mit vernünftigem Aufwand zu entschlüsseln.

Verwendung von Public Key Krypto-Systemen

Public Key Krypto-Systeme . . .

- sind in der Regel langsamer als symmetrische Verfahren.
- werden vor allem benutzt zum sicheren Schlüsselaustausch (danach: meist Anwendung von symmetrischen Verfahren).

Diskreter Logarithmus

- Zentrale Annahme für die Sicherheit von vielen Kryptosystemen: Diskreter Logarithmus ist schwierig zu bestimmen.

Diskreter Logarithmus – Definition

- **Recap – reelle Zahlen:**
  $\log_a(z)$ bezeichnet die Lösung der Gleichung $a^x = z$.
  (Bsp: $\log_2(1024) = 10$, da $2^{10} = 1024$)

Definition

Wir betrachten die Gruppe $\mathbb{Z}_n^*$. Für gegebene $a, z \in \mathbb{Z}_n^*$ bezeichnet

$$\log_a(z)$$

die Lösung der Gleichung $a^x = z \pmod{n}$

1. **Bemerkung:** Der obige Ausdruck heisst **diskreter** Logarithmus.

Beispiele: Wir setzen $n = 11$. (D.h. wir betrachten $\mathbb{Z}_{11}^*$.)

- $\log_6(9) = ?$, $\log_7(5) = ?$

Diskreter Logarithmus – Beispiel

- **Aufgabe:** Vervollständigen Sie die untenstehenden Tabellen, welche die 2-er und 3-Logarithmen in $\mathbb{Z}_{11}^*$ beinhalten:

$a =$	1	2	3	4	5	6	7	8	9	10
$\log_2(a)$										

$a =$	1	2	3	4	5	6	7	8	9	10
$\log_3(a)$										

Empfehlung: Arbeiten Sie hier nur mit der Exponentialfunktion.

Diskreter Logarithmus – Eigenschaften

Bemerkungen

- Es gibt Konstellationen, in denen der diskrete Logarithmus nicht existiert (s. vorherige Tabelle).
- Ist die Basis ein **erzeugendes Element**, so existieren alle zugehörigen diskreten Logarithmen (s. Tabelle mit $\log_2(a)$).
- zugehöriger Befehl in PARI/GP: `znlog`
  (Beispiel-Eingabe für die Berechnung von $\log_2(5)$:
  $a = \mathrm{Mod}(2, 11)$, $b = \mathrm{Mod}(5, 11)$, $\mathrm{znlog}(b, a)$)

Diffie Hellman Schlüssel-Austausch

Alice		Bob
	gemeinsame Wahl von p und Erzeugendes $g \in Z_p^*$ $\longleftrightarrow$	
1. wähle geheim $a \in Z_p^*$		wähle geheim $b \in Z_p^*$
2. $A := g^a \pmod{p}$		$B := g^b \pmod{p}$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
3. key $= B^a$		3. key $= A^b$

Bem:

- $B^a = (g^b)^a = g^{ab}$
- $A^b = (g^a)^b = g^{ab}$

$\Rightarrow$ key $= g^{ab}$

Diffie Hellman Schlüssel-Austausch

- **Aufgabe:** Spielen Sie den Diffie Hellman Austausch durch für $p = 11$, $g = 2$, $a = 5$ und $b = 7$.