Inhalt

Diffie Hellman Schlüssel-Austausch

Recap: Schlüssel-Austausch in $\mathbb{Z}_p^*$:

Alice	gemeinsame Wahl von p und Erzeugendes $g \in Z_p^*$ $\longleftrightarrow$	**Bob**
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 $= g^{ab}$

Bem: Wechsel zu ell. Kurven: Exponenten werden zu Faktoren!

Schlüssel-Austausch für elliptische Kurven:

Alice	gemeinsame Wahl von P (Punkt grosser Ordnung) $\longleftrightarrow$	**Bob**
1. wähle geheim k_A		wähle geheim k_B
2. $A := k_A \cdot P$		$B := k_B \cdot P$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
3. key $= k_A \cdot B$		3. key $= k_B \cdot A$

Bem:

- $k_A \cdot B = k_A \cdot (k_B \cdot P) = (k_A \cdot k_B) \cdot P$
- $k_B \cdot A = k_B \cdot (k_A \cdot P) = (k_B \cdot k_A) \cdot P$

$\Rightarrow$ key $= (k_A \cdot k_B) \cdot P$

Diffie Hellman Schlüssel-Austausch

Aufgabe: Wir betrachten die folgenden Grössen:

- $E : y^2 = x^2 + 3x + 2$
- $K = \mathrm{GF}(23)$
- $P = (0, 5)$ (Hinweis: Dieses Element von E hat Ordnung 28.)
- $k_A = 3$, $k_B = 9$

Bestimme den gemeinsamen Schlüssel.

El Gamal Verschlüsselung

Recap: Verschlüsselung in $\mathbb{Z}_p^*$:

Alice

1. Schlüssel-Erzeugung
   - wähle p,g
   - wähle geheim $a \in Z_p^*$
   - $A := g^a \pmod{p}$

$$\xrightarrow{\quad A \quad}$$

Bob

2. Verschlüsselung
   - $m :=$ Nachricht
   - wähle geheim $b \in Z_p^*$
   - $B := g^b \pmod{p}$
   - $c := A^b \cdot m \pmod{p}$

$$\xleftarrow{\quad (B, c) \quad}$$

3. Entschlüsselung
   - $m := c \cdot B^{p-1-a}$

Bem: Ell. Kurven: Exponent $\rightsquigarrow$ Faktor, Multiplikation $\rightsquigarrow$ Addition!

El Gamal Verschlüsselung

Verschlüsselung für elliptische Kurven:

Alice		**Bob**
1. Schlüssel-Erzeugung • wähle $K = \mathrm{GF}(p)$ • wähle ell. Kurve E • wähle Punkt P auf E • wähle geheim k_A • $A := k_A \cdot P$		
	$\xrightarrow{(E, p, P, A)}$	
		2. Verschlüsselung • $M :=$ Nachricht • wähle geheim k_B • $B := k_B \cdot P$ • $C := M + k_B \cdot A$
	$\xleftarrow{(B, C)}$	
3. Entschlüsselung • $M := -k_A \cdot B + C$		

El Gamal Verschlüsselung

Wir betrachten die folgenden Grössen:

- $E : y^2 = x^3 + 3x + 9$
- $K = \mathrm{GF}(11)$
- $P = (2, 1)$ (Hinweis: Dieses Element von E hat Ordnung 11.)
- $k_A = 7$, $k_B = 3$
- $M = (10, 4)$

Spiele Verschlüsselung und Entschlüsselung durch unter Verwendung der PARI-GP Befehle **ellinit**, **ellpow**, **elladd**.

Nachricht $\rightarrow$ Punkt auf elliptischer Kurve

- Annahme: Nachricht ist als Ganz-Zahl repräsentiert (Standard).
- Verbleibende Problemstellung:
  Transformation Nachricht $\rightarrow$ Punkt auf elliptischer Kurve?

Nachricht → Punkt auf elliptischer Kurve

- Vorgegeben: elliptischen Kurve E der Form: E: $y^2 = x^3 + ax + b$

Input: Nachricht m (dargestellt als ganze Zahl)

Output: Punkt (x, y) auf E mit der Eigenschaft $m = \left\lfloor \frac{x}{128} \right\rfloor$

MessageToPoint(m)
    $j := 0$
    while ($j \leq 127$)
        { $x := 128m + j$
        if ($x > p$) **return** ("leider keinen Punkt gefunden")
        $s := x^3 + ax + b$
        prüfe, ob s quadratischer Rest modulo p ist
        falls ja:
            finde y mit $y^2 = s$
            return (x, y)
        $j := j + 1$ }
    return ("leider keinen Punkt gefunden")
end

Input: Punkt (x, y) (dargestellt als ganze Zahl)

Output: Nachricht m mit der Eigenschaft $m = \left\lfloor \frac{x}{128} \right\rfloor$

POINTTOMESSAGE((x, y))

$$m := \left\lfloor \frac{x}{128} \right\rfloor$$

end

Nachricht $\to$ Punkt auf elliptischer Kurve

- **Frage:** Was spricht für die Wahl der Zahl 128?
  (anstelle von – z.B. 127 oder 129)
- **Aufgabe:** Wir betrachten die Kurve E: $y^2 = x^3 + 3x + 5$ über GF(10'009).
  - (i) Stelle die Nachricht $m = 10$ als Punkt M der elliptischen Kurve dar.
  - (ii) Gebe an, wie aus dem Punkt M die Nachricht m rekonstruiert wird.

  Tipp: Wurzel-Abfrage resp. Bestimmung geht mithilfe der PARI/GP-Befehle `issquare` resp. (...)^(1/2)