ÜBUNG

Verschlüsseln Sie mit dem DSA-Algorithmus den Klartext $M = 10$ mit den Parametern $p = 29$, $q = 31$ und $e =$ ~~###~~ Führen Sie auch eine adäquate Entschlüsselung durch. $e = 13$

Lösung der Übung vom Wiedemann siehe letzte Seiten
(in schwarz geschrieben)

$$n = p \cdot q = 29 \cdot 31 = 899$$

$$\phi(n) = \phi(899) = 28 \cdot 30 = 840$$

[sagt aus: Von den 899 Zahlen 0 bis 898 haben 840 ein multiplikatives Inverses mod 899]

Vorgegeben $e = 13$ mit $ggT(e, \phi(n)) = ggT(13, 840) = 1$

dadurch ist gewährleistet, dass $d = e^{-1}$ existiert.

Berechnung über den erweiterten EUKLID.

$x_1 \leftarrow 1$	$y_1 \leftarrow 0$	$13^{-1} \bmod 840$
$x_2 \leftarrow 0$	$y_2 \leftarrow 1$	
$x_3 \leftarrow 840$	$y_3 \leftarrow 13$	

$$Q = \left\lfloor \frac{x_3}{y_3} \right\rfloor = \left\lfloor \frac{840}{13} \right\rfloor = 64$$

$x_1 \leftarrow 2$ $\quad y_1 \leftarrow -3$

$x_2 \leftarrow -129$ $\quad y_2 \leftarrow 194$

$x_3 \leftarrow 3$ $\quad y_3 \leftarrow 2$

$Q = 1$

$T_1 = 2 + 3 = 5$

$T_2 = -129 - 194 = -323$

$T_3 = 1$

↯ STOP

$13^{-1} \bmod 840 = -323 \bmod 840$

$\equiv 517 \bmod 840$

⇒ Checke: $13 \cdot 517 = 6720 + 1$

$= 8 \cdot 840 + 1$

$\equiv 1 \bmod 840$

⇒

$K_{pub} = (e, n) = (13, 899)$

$K_{priv} = (d, n) = (517, 899)$

Verschlüsselung

$C = M^e \bmod n$

$= 10^{13} \bmod 899$

$= (10^8 \cdot 10^4 \cdot 10) \bmod 899$

$= \underline{722}$

$10^2 \mod 899 = 100 \mod 899$

$10^4 \mod 899 \equiv 111 \mod 899$

$10^8 \mod 899 \equiv 634 \mod 899$

$\downarrow$ $10^{13} \mod 899 = (634 \cdot 111 \cdot 10) \mod 899$

$\equiv 722 \mod 899$

Analog:

$$M = C^d \mod n = 722^{517} \mod 899$$

$$\vdots$$

$$= 10$$

$$722^{517} = 722^{512} \cdot 722^4 \cdot 722$$

$$= 732 \cdot 516 \cdot 722$$

Das DIFFIE-HELLMAN Key-Exchange Verfahren

Dieses Verfahren wurde in der Arbeit

"New Directions in Cryptography"

vorgestellt, zählt zu den Public-Key Verfahren, ermöglicht aber

- keine Verschlüsselung
- keine digitale Signatur.

Generell nützen Public-Key-Verfahren sogenannte Trapdoor-Funktionen, das sind Funktionen, die in der einen Richtung einfach sind, die Umkehrung jedoch schwierig bis unmöglich.

RSA: $p, q \xrightarrow{\text{einfach}} n = p \cdot q$

$\xleftarrow{\text{schwierig}}$

Eine andere Trapdoor-Funktion ist z.B.

→ Berechne $\prod_{i=1}^{11} (x - i) = (x-1)(x-2)\cdot(x-3)\cdots(x-11)$

$= x^{11} - 66x^{10} + 1925x^9$

$- 32670x^8 + 35742 \cdot x^7$

$\ldots - 39916800.$

Das DH-Key-Exchange Verfahren nutzt den diskreten Logarithmus als Trapdoor-Funktion, d.h. die Sicherheit des DH-Verfahrens hängt davon ab, dass es sehr schwierig ist (bis unmöglich) diskrete Log. zu berechnen.

Betrachte wieder die Menge $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$.
Eine primitive Wurzel einer Primzahl p ist eine Zahl in $\mathbb{Z}_p \setminus \{0\}$, deren Potenzen alle Zahlen von 1 bis $p-1$ generiert. Ist a eine primitive Wurzel, dann sind

$$a \bmod p,\ a^2 \bmod p,\ a^3 \bmod p,\ \ldots,\ a^{p-1} \bmod p$$

alle unterschiedlich und bestehen aus den Zahlen 1 bis $p-1$ in irgend einer (wilden!) Reihenfolge.

Beispiel: $p = 13$ $\quad a = 2$

$2^1 \bmod 13 = 2$

$2^2 \bmod 13 = 4$

$2^3 \mod 13 = 8$

$2^4 \mod 13 = 5$

$2^5 \mod 13 = 10$

$2^6 \mod 13 = 7$

$2^7 \mod 13 = 1$

~~$a = 2$~~

$2^8 \mod 13 =$

$p = 13, \quad a = 3$

$3^1 \mod 13 = 3$

$3^2 = 9$ ist's nicht

$3^3 = 1$

$p = 13 \qquad a = 5$

$5 \mod 13 = 5$

$5^2 = 12$

$5^3 = 9$

$5^4 = 6$

$5^5 = 4$

$5^6 = 7$

$5^7 = 9$

$p = 7 \qquad a = 3$

$p = 7 \quad 1, 2, 3, 4, 5, 6$

$\mathbb{Z}_7^* \{ \}$

$3^1 \mod 7 = 3$

$3^2 \mod 7 = 2$

$3^3 \mod 7 = 6$

$3^4 \mod 7 = 4$

$3^5 \mod 7 = 5$

$3^6 \mod 7 = 1$

Das diskrete Logarithmusproblem besteht:

Finde i mit

$$b = a^i \bmod p \qquad 0 \leq i \leq p-1$$

i heisst diskreter Log. – oder Index – von b für die Basis $a \bmod p$.

$$\boxed{i = \mathrm{ind}_{a,p}(b)}$$

Das DH – Key – Exchange Kryptosystem

(1) Szenario

Alice und Bob wollen einen gemeinsamen Schlüssel erzeugen, den nur sie kennen, ohne sich zuvor begegnet zu sein.

(2) Alice und Bob einigen sich (öffentlich) auf eine Primzahl q und eine primitive Wurzel a. (q, a ist eine Art Public Key)

(3) Geheimer Schlüssel Alice

Alice wählt eine Zahl X_A $X_A < q$ und nur Alice kennt. Alice berechnet

$$Y_A = a^{X_A} \bmod q$$

Y_A wird an Bob gesendet.

(4) Geheimer Schlüssel Bob

Bob wählt eine Zahl X_B $X_B < q$ nur Bob kennt

Bob berechnet

$$Y_B = a^{X_B} \bmod q.$$

Y_B geht an Alice.

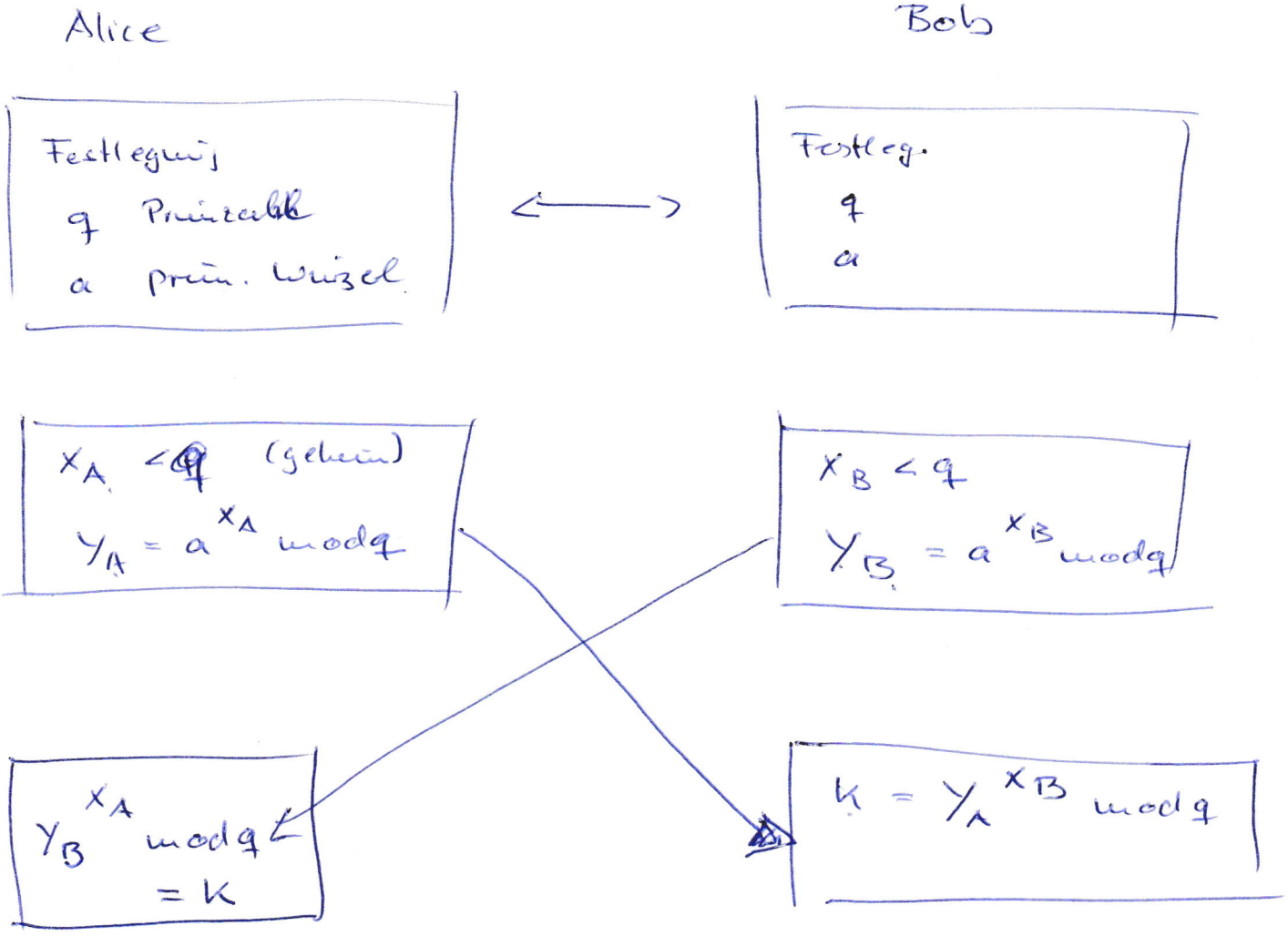
(5) Alice berechnet:

$$K = (Y_B)^{X_A} \bmod q$$

(6) Bob berechnet

$$K' = (Y_A)^{X_B} \bmod q$$

→ da $K = K'$ (gleich) haben Bob und Alice einen gemeinsamen Sitzungsschlüssel.



Es gilt:

$$K = Y_B^{X_A} \bmod q \qquad \text{(Alice)}$$

$$= (a^{X_B} \bmod q)^{X_A} \bmod q$$

$$= (a^{X_B})^{X_A} \bmod q$$

$$= a^{x_B \cdot x_A} \mod q$$

$$= (a^{x_A})^{x_B} \mod q$$

$$= y_A^{x_B} \mod q = k' \text{ von Bob}$$

Also: öffentlich: q, a, y_A, y_B

Ein Angreifer, der den Schlüssel k erhalten will muss x_A oder x_B berechnen aus:

$$y_A = a^{x_A} \mod q$$

oder $$y_B = a^{x_B} \mod q$$

oder $$x_B = \text{ind}_{a,q}(y_B)$$

DH-Verfahren macht nur Sinn, wenn beide Parteien 'online' sind, denn Alice und Bob müssen eine Reihe von Informationen austauschen (q, a, x_A, y_B) bevor kommuniziert wird.

Beispiel: Alice und Bob einigen sich auf

$$q = 479, \quad a = 11$$

Alice wählt $x_A = 102$ $\quad 1 \leq x_A \leq 478$

Bob wählt $x_B = 110$. $\quad x_B$

Alice berechnet $y_A = a^{x_A} \mod q$

$$= 11^{102} \mod 479$$

fastexp $= 218$

$218 = Y_A$ wird an Bob gesendet.

Bob berechnet $Y_B = a^{x_B} \bmod q$

$= 11^{110} \bmod 479$

fastexp $\vdots$

$= \underline{\underline{42}}$ → an Alice

Dann berechnet Alice

$K_1 = Y_B^{x_A} \bmod q$

$= 42^{102} \bmod 479$

fastexp $\vdots$

$= \underline{\underline{242}}$

Bob berechnet:

$K' = Y_A^{x_B} \bmod q$

$= 218^{110} \bmod 479$

fastexp $\vdots$

$= \underline{\underline{242}}$ Session key $\underline{\underline{K = 242}}$

ELGAMAL - Kryptosystem (TAHER ELGAMAL, 1985)

digitale Signatur

Schlüssel: Wähle eine Primzahl p und zwei Zufallszahlen g, x mit $g, x < p$.

Berechne $y = g^x \bmod p$.

$k_{pub} = [y, g, p]$

$k_{priv} = [x]$

~~Digit~~ Signatur: M soll signiert werden.

Wähle zufällige Zahl k, so dass $k, p-1$ coprim sind, d.h.

$$ggT(k, p-1) = 1$$

Berechne $a = g^k \bmod p$.

Berechne b aus

$$M \equiv (xa + k \cdot b) \bmod (p-1)$$

Signatur (a, b), k geheim.

Bob verifiziert die Signatur wie folgt. M

es muss gelten:

$$y^a a^b \bmod p \overset{!}{=} g^M \bmod p.$$

Bsp: ① $p = 13$ $g = 7$ öffentliche Zahlen.

② Alice wählt als geheimen $k_{priv} = x = 3$

③ $y = g^x \bmod p = 7^3 \bmod 13 = 5$

$$k_{pub}^{A} = [p, g, y] = [13, 7, 5]$$

$$k_{priv}^{A} = [x] = [3]$$

Klartext, der von Alice signiert wird, ist $M = 10$

Zum Signieren muss Alice die Zahlen a, b bestimmen.

→ ④ Alice wählt zufällig Zahl $k = 5$,

ist ok, $ggT(5, 12) = 1$

⑤ $a = g^k \bmod p$

$= 7^5 \bmod 13 \equiv 11 \bmod 13$

⑥ Berechne b aus

$$M = (x \cdot a + k \cdot b) \bmod (p-1)$$

$$10 = (3 \cdot 11 + 5 \cdot b) \bmod 12$$

$$= (9 + 5 \cdot b) \bmod 12$$

$$\Leftrightarrow \quad 1 \equiv 5 \cdot b \bmod 12$$

$$\Rightarrow \quad \underline{\underline{b = 5}}$$

An Bob wird gesendet

→ Klartext $M = 10$

→ Signatur wurde $[a, b] = [11, 5]$

→ K_{pub} von Alice, $K^A_{pub} = [p = 13, g = 7, y = 5]$

Verifikation:

$$(y^a \cdot a^b) \bmod p \overset{!}{=} g^M \bmod p.$$

links: $(5^{11} \cdot 11^5) \bmod 13 = 4 \bmod 13$

rechts $7^{10} \bmod 13 = 4 \bmod 13$

⇒ beide Terme sind gleich → Alice hat die Nachricht gesendet.

Lösung der Übung zum RSA-Algorithmus vom Wiedemann

$n = 29 \cdot 31 = 899$

$k_{pub} = (13, 899)$

$\phi(n) = 840$

gesucht: $13^{-1} \bmod 840$

$x_1 \leftarrow 1$ $\quad y_1 \leftarrow 0$

$x_2 \leftarrow 0$ $\quad y_2 \leftarrow 1$

$x_3 \leftarrow 840$ $\quad y_3 \leftarrow 13$

$$Q = \left\lfloor \frac{840}{13} \right\rfloor = 64$$

$T_1 = x_1 - Q y_1 = 1$

$T_2 = x_2 - Q y_2 = -64$

$T_3 = x_3 - Q y_3 = 8$

$x_1 \leftarrow 0$ $\quad y_1 \leftarrow 1$

$x_2 \leftarrow 1$ $\quad y_2 \leftarrow -64$

$x_3 \leftarrow 13$ $\quad y_3 \leftarrow 8$

$$Q = \left\lfloor \frac{13}{8} \right\rfloor = 1$$

$T_1 = x_1 - Q y_1 = -1$

$T_2 = x_2 - Q y_2 = 65$

$T_3 = 13 - 8 = 5$

$x_1 \leftarrow 1$ $\quad y_1 \leftarrow -1$

$x_2 \leftarrow -64$ $\quad y_2 \leftarrow 65$

$x_3 \leftarrow 8$ $\quad y_3 \leftarrow 5$

$Q = 1$

$T_1 = 1 + 1 = 2$

$T_2 = -64 - 65 = -129$

$T_3 = 3$

$x_1 \leftarrow -1$ $\quad y_1 \leftarrow 2$

$x_2 \leftarrow 65$ $\quad y_2 \leftarrow -129$

$x_3 \leftarrow 5$ $\quad y_3 \leftarrow 3$

$Q = 1$

$T_1 = -1 - 2 = -3$

$T_2 = 65 + 129 = 194$

$T_3 = 2$

$x_1 \leftarrow 2$ $\quad y_1 \leftarrow -3$

$x_2 \leftarrow -129$ $\quad y_2 \leftarrow 194$

$x_3 \leftarrow 3$ $\quad y_3 \leftarrow 2$

$Q = 1$

$T_1 = 2 + 3 = 5$ $\qquad T_3 = 1$

$T_2 = -129 - 194 = -323$

↓ $d \equiv 13^{-1} \bmod 840 = -323$

$\equiv 517$

$13 \cdot 517 = 6720 + 1$

$= 8 \cdot 840 + 1$ ✓

$k_{priv} = (517, 899)$

$M = 10$

$C = 10^{13} \bmod 899$

~~$= 10 \cdot$~~ $10^2 \bmod 899 = 100$

$10^4 \bmod 899 = 111$

$10^8 = 634$

$C = (634 \cdot 111 \cdot 10) \bmod 899$

$= 722$

$722^{517} \mod 899$

$= \left(722^{512} \cdot 722^{4} \cdot 722 \right) \mod 899$

$722^2 = 763$

$722^4 = 516$

$722^8 = 152$

$722^{16} = 629$

$722^{32} = 81$

$722^{64} = 268$

$722^{128} = 803$

$722^{256} = 226$

$722^{512} = 732$

$732 \cdot 516 \cdot 722 = 10$

$T_1 = X_1 - Q Y_1 = 1$

$T_2 = X_2 - Q Y_2 = -64$

$T_3 = X_3 - Q Y_3 = 8$

$X_1 \leftarrow 0$ $\quad$ $Y_1 \leftarrow 1$

$X_2 \leftarrow 1$ $\quad$ $Y_2 \leftarrow -64$

$X_3 \leftarrow 13$ $\quad$ $Y_3 \leftarrow 8$

$$Q = \left\lfloor \frac{13}{8} \right\rfloor = 1$$

$T_1 = X_1 - Q Y_1 = -1$

$T_2 = X_2 - Q Y_2 = 65$

$T_3 = 5$

$X_1 \leftarrow 1$ $\quad$ $Y_1 \leftarrow -1$

$X_2 \leftarrow -64$ $\quad$ $Y_2 \leftarrow 65$

$X_3 \leftarrow 8$ $\quad$ $Y_3 \leftarrow 5$

$$Q = 1$$

$T_1 = X_1 - Q Y_1 = 2$

$T_2 = -64 - 65 = -129$

$T_3 = 8 - 5 = 3$

$X_1 \leftarrow -1$ $\quad$ $Y_1 \leftarrow 2$

$X_2 \leftarrow 65$ $\quad$ $Y_2 \leftarrow -129$

$X_3 \leftarrow 5$ $\quad$ $Y_3 \leftarrow 3$

$$Q = 1$$

$T_1 = X_1 - Q Y_1 = -3$

$T_2 = X_2 - Q Y_2 = 194$

$T_3 = 2$