

ggT(1761, 50) Krypto-Klausur 10.7.07

a)  $1761 = 35 \cdot 50 + 11$   $1 = 9 \cdot 1761 + 317 \cdot 50$   
 $50 = 4 \cdot 11 + 6$   $1 = 2 \cdot 50 + 9 \cdot (-1761 + 35 \cdot 50)$   
 $11 = 1 \cdot 6 + 5$   $1 = 2 \cdot 50 + 9 \cdot 11$   
 $6 = 1 \cdot 5 + 1$   $1 = -1 \cdot 11 + 2 \cdot (50 - 4 \cdot 11)$   
 $1 = -1 \cdot 11 + 2 \cdot 6$   
 $1 = 6 - 1 \cdot (11 - 1 \cdot 6)$   
 $1 = 6 - 1 \cdot 5$

$1 \equiv -9 \cdot 1761 + 317 \cdot 50$   
 $\quad \quad \quad 1761$

b)  $1 \equiv 0 + 317 \cdot 50$   
 $\quad \quad \quad 1761$   
 317 ist der Inverse von 50 mod 1761

~~ggT~~  $(1761 = 3 \cdot 587)$

d)  $480 = 6 \cdot 8 \cdot 10 = 2 \cdot 3 \cdot 2^3 \cdot 2 \cdot 5 = 2^5 \cdot 3 \cdot 5$

d)  $504 = 9 \cdot 56 = 9 \cdot 7 \cdot 8 = 2^3 \cdot 3^2 \cdot 7$

ggT(480, 504)  $\equiv 2^4$  jeder germin vorne Platz

kgV(480, 504)  $= 2^5 \cdot 3^2 \cdot 5 \cdot 7 = 10080$   
 jeder platz

- 2) a)  $(\mathbb{Z}_n, +)$  ist für alle  $n \in \mathbb{N}$  Gruppe  
 b)  $(\mathbb{Z}_n, +, \cdot)$  ist für Nicht-Primzahlen (für Zerlegbar.)  
 nur Ring, denn dann ex.  $a, b$  mit  $n = a \cdot b$ ,  
 aber  $a \cdot b \equiv 0 \pmod n$ ,  $a, b$  sind Nullteiler und  
 haben kein Inverses.  $(\mathbb{Z}_p, +, \cdot)$  ist Körper für  
 $p$  prim.

c)  $\mathbb{Z}_n^*$  ist die Menge der sup teilerfremden  
 Zahlen <sup>mit</sup> kleiner  $n$ . Es sind  $\varphi(n)$  Elemente  
 daran. Wie groß  $\varphi$  im einzelnen ist ist nicht  
 allgemein zu sagen  $n = p \cdot q \Rightarrow \varphi(n) = (p-1)(q-1)$

d)  $\mathbb{Z}_6^* = \{1, 5\}$ 

1 5	Gruppentafel	5+5 $\equiv$ 4 $\notin \mathbb{Z}_6^*$
5 1		

  
 die 1 für 2 El.



# Kryptiklausur 10.7.07 Diffie-Hellman

④  $p=13 \quad g=2$

$(2, 6, 7, 11)$

✓ = eigene Wahl

b) Anton

$a=5$  ✓

$2^5 \bmod 13 = 6 = \alpha \cdot g$

Berta

$b=10$  ✓

$2^{10} \bmod 13 = 10 = \beta$

5

$10^5 \bmod 13 = 4 = k_a$

$6^{10} \bmod 13 = 4 = k_b$

4

Also  $k_a = 4 = k_b$

c)  $k_a = \beta^a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = \alpha^b = k_b$  4  
 Rechnung in  $\mathbb{Z}_p^*$  qed

d) 8 ist keine Primzahl = erzeugendes Element.  
 nach 3c) Wählt Anton  $a=4$  und Berta  $b=3$   
 so werden sie beide  $\alpha=1, \beta=1 \Rightarrow k_a=k_b=1$   
 und es ist kein vernünftiger Schlüssel. 4

Sie merken das ja aber schon aus Rechnung und  
 müssen dann of von vornherein. Übersicht  
 und bei ~~2~~ 3

⑤  $s=31128793$

$c=50348543$

$c=81466236$

$s+m=c \bmod 10$   
 $5 \rightarrow 8 \quad 5+3 \equiv 8$

$c \begin{matrix} 12 \\ 276 \\ -5503 \\ \hline m 773 \end{matrix}$

ja, man kann modulo 10  
 addieren, denn die Tabelle  
 ist die Gruppentafel  $(\mathbb{Z}_{10}, +)$

$c \equiv m+s$

$m \equiv c-s$

$c-s \equiv m$   
 $2-5 \equiv -3 \equiv 7$

Oder  $2-5 \equiv 12-5 = 7$

↳ darum ist auch  
 Abziehen stets  
 möglich.

Kynpbe  
 Ac 7.07  
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35

1) a) EA vor 2 mid 3  
 b) Struktur  
 c) 480 = "

2) a) 504 = Sept. 65 Takt  
 b) 12 n + 1 Gm  
 c) nur Baum's, K0  
 d)  $\sum_{i=1}^n G_i + 7$

3) a) 072, 08, Prod. = 12 3/4  
 b) Prod. und. Prod.  
 c) < 88, 2 (88) 4 (88)  
 d) Seite  
 e) 8 mo mod 13  
 f) Bsp. mit 8=3 8=5

4) a) b) Wert von was  
 c) Durchschnittswert  
 d) g. Primzahl konstant  
 e) Wahrscheinlichkeit

5) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

6) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

7) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

8) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

9) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

10) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

11) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

12) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

13) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

14) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

15) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

16) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

17) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

18) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

19) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

20) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

21) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)

22) a) b) c) d) e) f) g) h) i) j) k) l) m) n) o) p) q) r) s) t) u) v) w) x) y) z)