

Aufgabe 38

$$\begin{aligned}
 g &= 3 \\
 A = 30 &= 3^{11} \pmod{43} \Rightarrow a = 11 \\
 B = 24 &= 3^{40} \pmod{43} \Rightarrow b = 40 \\
 K = g^{a \cdot b} &\pmod{43} = 3^{11 \cdot 40} \pmod{43} = 14
 \end{aligned}$$

Die vorgeschlagene Tabelle wurde via Perl-Skript generiert :

`./uebung11.pl 38`

Aufgabe 39

Der private Schlüssel ist 11 (wie schon in Aufgabe 38 herausgefunden, $b = 30 = 3^a \pmod{43} \Rightarrow a = 11$), der Klartext somit $d_K(24, 7) = 7 \cdot (24^{11})^{-1} \pmod{43} = 22$. Dieses Ergebnis wurde mittels Perl-Skript ermittelt :

`./uebung11.pl 39`

Aufgabe 40

$$\begin{aligned}
 g &= 3 \\
 n &= |\mathbb{Z}_{353}^*| = 352 \text{ (da 353 prim)} \\
 m &= \lceil \sqrt{n} \rceil = \lceil \sqrt{352} \rceil = 19 \\
 d &= g^m = 3^{19} \pmod{353} = 142 \\
 L_{1\text{unsortiert}} &= \begin{matrix} (0,1) & (1,142) & (2,43) & (3,105) & (4,84) & (5,279) & (6,82) \\ (7,348) & (8,349) & (9,138) & (10,181) & (11,286) & (12,17) & (13,296) \\ (14,25) & (15,20) & (16,16) & (17,154) & (18,335) \end{matrix} \\
 L_{2\text{unsortiert}} &= \begin{matrix} (0,143) & (1,283) & (2,212) & (3,306) & (4,102) & (5,34) & (6,129) \\ (7,43) & (8,132) & (9,44) & (10,250) & (11,201) & (12,67) & (13,140) \\ (14,282) & (15,94) & (16,149) & (17,285) & (18,95) \end{matrix} \\
 L_1 &= \begin{matrix} (0,1) & (16,16) & (12,17) & (15,20) & (14,25) & (2,43) & (6,82) \\ (4,84) & (3,105) & (9,138) & (1,142) & (17,154) & (10,181) & (5,279) \\ (11,286) & (13,296) & (18,335) & (7,348) & (8,349) \end{matrix} \\
 L_2 &= \begin{matrix} (5,34) & (7,43) & (9,44) & (12,67) & (15,94) & (18,95) & (4,102) \\ (6,129) & (8,132) & (13,140) & (0,143) & (16,149) & (11,201) & (2,212) \\ (10,250) & (14,282) & (1,283) & (17,285) & (3,306) \end{matrix} \\
 x &= (19 \cdot 2 + 7) \pmod{352} = 45 \text{ (Probe : } 3^{45} \equiv 143 \pmod{353}\text{)}
 \end{aligned}$$

Somit ist $x = 45$ mittels des Babystep-Giantstep-Algorithmus von Shanks gefunden.

Aufgabe 41

Das Ergebnis wurde via Perl-Skript ermittelt :

```
./uebung11.pl 41
```

443 Iterationen, Kollision bei $(b_i = 339768, y_i = 22811, z_i = 35067), (b_{2i} = 339768, y_{2i} = 37251, z_{2i} = 5360)$.

$ggT(z_{2i} - z_i, n) = 1$, somit $x = (y_i - y_{2i}) \cdot (z_{2i} - z_i)^{-1} \pmod n = -14440 \cdot 27580 \pmod n = 40007$

Aufgabe 42 wird auf einem separaten Blatt abgegeben.

Anhang 38-42

```
#!/usr/local/bin/perl -w
use strict; no strict 'refs'; use Math::BigInt;

sub extended_euclid {
    $_[1] or return $_[0], 1, 0;
    my ($d, $x, $y) = extended_euclid ($_[1], $_[0] % $_[1]);
    $d, $y, $x - $y * ($_[0] / $_[1])
}

sub loese_mod_eq {
    my ($d, $x, $y) = extended_euclid ($_[0], $_[2]);
    $_[1] % $d ? undef : map { ($x * $_[1] / $d % $_[2] + $_ * $_[2] / $d)
        % $_[2] } 0..$d-1
}

sub prob38 {
    print "3^$_%43=", (new Math::BigInt(3)**$_)%43, "\n" for 0..41
}

sub elGamal {
    my ($y1, $y2, $a, $p) = @_;
    $y2*[loese_mod_eq(new Math::BigInt($y1)**$a, 1, $p)]->[0] % $p
}

sub prob39 {
    print elGamal (24, 7, 11, 43), "\n"
}

my ($p, $g, $n, $a) = map { new Math::BigInt($_) } 458009, 2, 57251, 56851;

sub f {
    my ($b, $y, $z) = @_;
    $b % 3 == 1 and return $a*$b%$p, $y, ($z+1)%$n;
}
```

```

    $b % 3 == 0 and return $b*$b%$p, 2*$y%$n, 2*$z%$n;
    $b % 3 == 2 and return $g*$b%$p, ($y+1)%$p, $z
}

sub prob41 {
    my ($b,$y,$z) = f map { new Math::BigInt ($_) } 1,0,0;
    my ($bs,$ys,$zs) = f $b,$y,$z; my $i;
    while ($b != $bs) {
        $i++;
        ($b,$y,$z) = f $b,$y,$z;
        ($bs,$ys,$zs) = f $bs,$ys,$zs;
        ($bs,$ys,$zs) = f $bs,$ys,$zs
    }
    print "$i Iterationen, Kollision bei \$(b_i=$b, y_i=$y, z_i=$z)",
          "(b_{2i}=$bs, y_{2i}=$ys, z_{2i}=$zs)\$.\\\\\\n";
    if ([extended_euclid ($zs-$z, $n)]->[0] == 1) {
        print '$ggT(z_{2i}-z_i, n) = 1$, somit ',
              '$x = (y_i-y_{2i}) \cdot (z_{2i}-z_i)^{-1} \pmod n = ', ($y-$ys),
              ' \cdot ', [loese_mod_eq($zs-$z,1,$n)]->[0], ' \pmod n = ',
              (($y-$ys)*[loese_mod_eq($zs-$z,1,$n)]->[0])%$n, "\$\\n";
    } else {
        print 'FAILURE, da $ggT(z_{2i}-z_i, n)$ \not= 1', "\n";
    }
}

&{'prob'.$ARGV[0]} (splice @ARGV,1)

```