1) $p = 107$

$g = 2 \pmod{107}$

$a = 66$

$b = 33$

$A = g^a \pmod{p} = 2^{66} \pmod{107} = 47$

$B = g^b \pmod{p} = 2^{33} \pmod{107} = 58$

$S_{Alice} = B^a \pmod{p} = 58^{66} \pmod{107} = 75$

$S_{Bob} = A^b \pmod{p} = 47^{33} \pmod{107} = 75$

} shared secret

2) $m = 9 \quad p = 31 \quad A = 17$

$b = 12 \quad g = 3 \quad a = 7$

$B = g^b = 3^{12} = 531441$

Verschlüsselung:

$c = A^b \cdot m = 17^{12} \cdot 9 = 5'243'600'135'067'849$

Entschlüsselung:

$m = c \cdot B^{(p-1-a)} \pmod{p} = c \cdot B^{31-1-7} \pmod{p} = c \cdot B^{23} \pmod{31} = 9$

3) $n = 59'153 \quad x_0 = 24'712 = y_0$

$a = 1$

$i = 1$

while no collision found:

$x_i = (x_i - 1)^2 + a \pmod n$

$y_i = ((y_i - 1)^2 + a)^2 + a \pmod n$

$d = ggT(x_i - y_i, n)$

if $(1 < d < n)$

return d

$i{+}{+}$

calculated using python

$d = 149$