RSA 1a)

$C = m^e \bmod n$

m = 0:

$C = 0^e \bmod n = 0 \bmod n = 0$

m = 1:

$C = 1^e \bmod n = 1 \bmod n = 1$

m = n - 1:

$C = (n - 1)^e \bmod n =$ 1, wenn e durch 2 teilbar
n - 1, sonst

$(n - 1)^2 \bmod n = n^2 - 2n + 1 \bmod n = 1$

$(n - 1)^3 \bmod n = (n - 1)^2 * (n - 1) \bmod n = (n - 1)^2 \bmod n * (n - 1) \bmod n$
$= 1 * (n - 1) \bmod n = n - 1$

3-partie-diffiehellmann

Gegeben 3 Kommunikationspartner (Pn), 1 öffentlicher Kommunikationskanal.

Öffentliche Einigung auf eine Primzahl n und einen Generator g:
Private zufällige Nummer für jeden Teilnehmer: x, y, z

P1 veröffentlicht: $X = g^x \bmod n$
P2 veröffentlicht: $Y = g^y \bmod n$
P2 veröffentlicht: $Z = g^z \bmod n$

P1 veröffentlicht:

1. $xY = Y^x \bmod n$
2. $xZ = Z^x \bmod n$

P2 veröffentlicht:

1. $yZ = Z^y \bmod n$

shared secret:
P3: $k = (xY)^z \bmod n = ((g^y)^x)^z \bmod n = g^{yxz} \bmod n$
P2: $k = (xZ)^y \bmod n = ((g^z)^x)^y \bmod n = g^{zxy} \bmod n$
P1: $k = (yZ)^x \bmod n = ((g^z)^y)^x \bmod n = g^{zyx} \bmod n$

RSA, DH 2b, 4b)
“kleine Zahlen - kleine Sicherheit” - Quelle VL 04