Verfahren am Beispiel (Alice möchte Bob eine geheime Botschaft schicken)

1. Bob erzeugt seinen **Privaten Schlüssel D** sowie seinen **Öffentlichen Schlüssel (N,E)** wie folgt:

P = 5 (P ist Primzahl, beliebig gewählt)
Q = 7 (Q ist auch beliebig gewählte Primzahl)

Festlegen von P, Q

N = 35 (N = P * Q)
M = 24 (M = (P-1) * (Q-1))

Berechnen von N, M

E = 5 (E mit E < N und ggT(E,M) = 1 wird bestimmt und festgelegt)
D = 5 (D wird festgelegt, so dass D * E mod M = 1,

Ermitteln von E, D

d.h. D * E – x * M = 1 für ein beliebiges, natürliches n)

2. Alice verschlüsselt ihre **Nachricht X** mit dem **Öffentlichen Schlüssel (N,E)** von Bob, genauer durch Anwenden der Formel **X^E mod N = X^5 mod 35** und erhält so die **verschlüsselte Nachricht Y.**

3. Bob entschlüsselt Y durch „Rückwärtsrechnen“ mit **Y^D mod N = Y^5 mod 35 = X**.

Beispiel:

DACH = 4-1-3-8 soll verschlüsselt werden:

4 ^5 mod 35 = 9 4^5=1024 |:35 = 29,26 | -29 (nur Kommaanteil=Rest) = 0,26 | *35 = 9
1 ^5 mod 35 = 1
3 ^5 mod 35 = 33
8 ^5 mod 35 = 8

Es ergibt sich also die Chiffre 9-1-33-8.

entschlüsseln:

9 ^5 mod 35 = 4
1 ^5 mod 35 = 1
33 ^5 mod 35 = 3 33^5=39135393|:35 = …,09 (gerundet)| 0,09*35=3,15
8 ^5 mod 35 = 8

Lösung: 4-1-3-8 = DACH ☺!

Natürlich ist das Verfahren in der Größenordnung der oben gewählten Primzahlen sehr unsicher! Man stelle sich vor ein Angreifer würde in den Besitz des Öffentlichen Schlüssels (N,E) = (35,5) gelangen (was recht einfach ist, da er öffentlich ist!). Dann könnte er aus der Gleichung 35=N=P*Q augenblicklich die Primzahlen P, Q und damit M folgern – genauer ergibt sich: P=5, Q=7 (oder umgekehrt, aber nicht von Belang) und demzufolge M=(P-1)*(Q-1)=24. Außerdem weiß er, dass D*E mod M = 1 gelten muss, also hier D*5 mod 24 = 1, woraus sich für D – durch Raten oder mit Hilfe des erweiterten Euklidischen Algorithmus mit M und E – z.B. folgende Zahlen ableiten lassen: 5, 29, 53, 77, … Allgemein ist D also ein Ergebnis der Summe aus 5 sowie einem Vielfachen von 24 (anders ausgedrückt: D = 5 + 24*x, wobei x eine beliebige natürliche Zahl darstellt). Es ist nun nicht schwer nachzuvollziehen, dass man recht schnell alle Möglichkeiten testweise entschlüsselnd durchspielen könnte..!

Weiteres theoretisches Beispiel:
P = 13, Q = 23, N = 13 * 23 = 299, M = 12 * 22 = 264
E < N = 299 und teilerfremd zu M = 264 = 2 * 2 * 2 * 3 * 11, also z.B. E = 5
D mit D * E mod M = 1, also D * 5 mod 264 = 1, also z.B. D = 53