Pollard für 10-bit

$p = 1019$ $\qquad q = \frac{p-1}{2} = 509$ Primzahl

$g = 2$ Erzeuger

$$2^x \equiv 7 \mod 1019$$

$q = 2$

$$\left(2^x\right)^{\frac{1019-1}{2}} \equiv 7^{\frac{1019-1}{2}} \mod 1019$$

$$1018^x \equiv 1018 \mod 1019$$

$$x \equiv 1 \mod 2$$

$q = 509$

$$\left(2^x\right)^{\frac{1019-1}{509}} \equiv 7^{\frac{1019-1}{509}} \mod 1019$$

$$4^x \equiv 49 \mod 1019$$

pollard (4, 49, 1019, 509)

↳ k, l, k2, l2

$$x \equiv \frac{k - k2}{l2 - l} \mod q$$

$$x \equiv 363 \mod 509$$

Chin. Restsatz

gp:

```
chinese(Mod(1,2),
    Mod(363,509))
```

Pollard für

24 bit

$p = 11309027$, $q = 5654513$

$g = 2$, $h = 7$

$$2^x \equiv 7 \bmod p$$

$$x \equiv 4\,313\,137 \bmod q$$