$N = 109$ $\quad 052|083|051|006|101|073|054|082|022$

$e = 47$ $\quad b = 1$

$E(m) = m^e \pmod N$ $\quad d = 23$

$D(c) = c^d \pmod N$

$$m^{\varphi(N)} = 1 \pmod N$$

$$D(E(m)) = m^{ed} \pmod N$$

$$ed \equiv 1 \pmod{\varphi(N)} \Rightarrow m^{ed} = m^{1+k\varphi(N)} \pmod N$$

$$d = e^{-1} \pmod{\varphi(N)} \qquad = m \cdot m^{k\varphi(N)} \pmod N$$

$$d = 47^{-1} \pmod{108} \qquad = m \pmod N$$

$$d \cdot 47 + k \cdot 108 = 1$$

$$d \cdot 47 + k \cdot 108 = \gcd(108, 47) \quad (=1)$$

$$108 = 2 \cdot 47 + 14$$

$$47 = 3 \cdot 14 + 5$$

$$14 = 2 \cdot 5 + 4$$

$$5 = 4 + 1$$

$$1 = -10 \cdot 108 + 23 \cdot 47$$

d

	108	47	
108	1	0	
47	0	1	$\times 1$
14	1	-2	$\times -3$ $+$
5	-3	7	$=$
4	7	-16	
1	-10	23	