Repeat Sqaring

(or Sqare-and-Multiply)

$m^e \pmod{n}$

①

$$e = 2$$
$$= (1\ 0)_2$$
$$m^e = \overset{\downarrow}{m^2}$$

②

$$e = 5$$
$$= (1\ 0\ 1)_2$$
$$m^e = (m^{\overset{\downarrow}{2}})^{\overset{\downarrow}{2}} \cdot m$$

③

$$e = 11$$
$$= (1\ 0\ 1\ 1)_2$$
$$m^e = ((m^{\overset{\downarrow}{2}})^{\overset{\downarrow}{2}} \cdot m)^{\overset{\downarrow}{2}} \cdot m$$

④

$e = 1235$

$= (1\,0\,0\,1\,1\,0\,1\,0\,0\,1\,1)_2$

$$m^e = (((((((((m^2)^2)^2 \cdot m)^2 m)^2)^2 m)^2)^2)^2 m)^2 m$$

Rule:

0 → sqare

1 → sqare then multiply