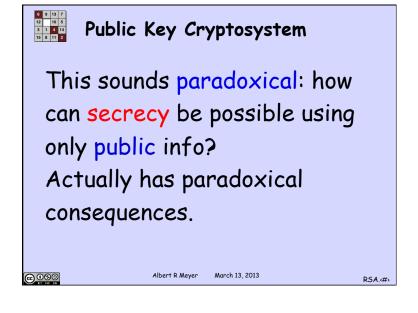


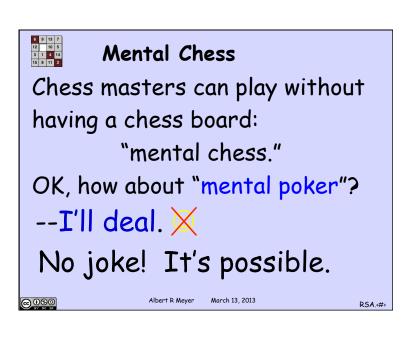
Albert R Mever March 13, 2013

RSA.1

 $\Theta$ 









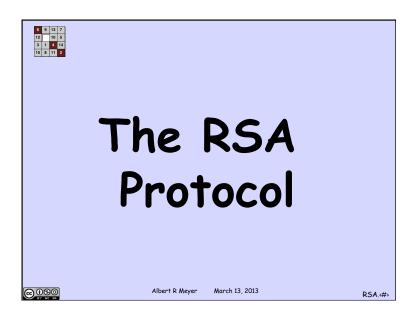
## One-way functions

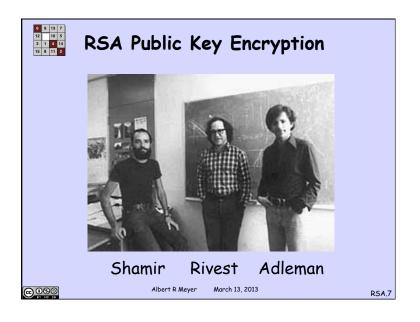
The paradoxical assumption is that there are one-way functions that are easy to compute but hard to invert. In particular,

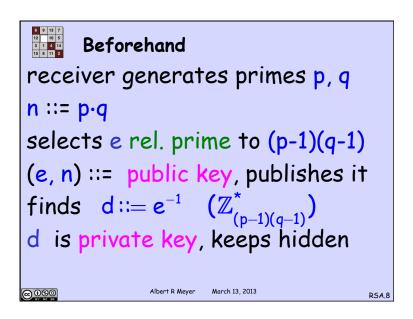
- it is easy to compute the product n of two (large) primes p and q.
- But given n, it is generally very hard to factor n to recover p and q

Albert R Mever March 13, 2013

RSA.«#»







```
Encoding message m \in [1,n)

send m^* := m^e (\mathbb{Z}_n)

Decoding m^*:

receiver computes

m = (m^*)^d (\mathbb{Z}_n)
```

