

Albert R Meyer

March 13 2013

@ 0 0 0



@ 000

Public Key Cryptosystem

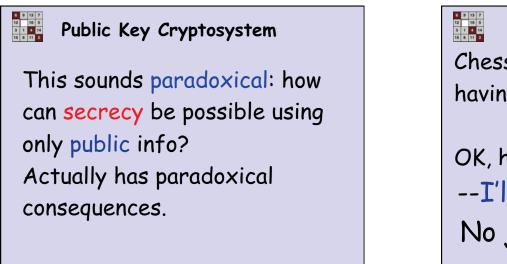
Anyone can send a secret (encrypted) message to the receiver, without any prior contact, using publicly available info.

March 13 2013

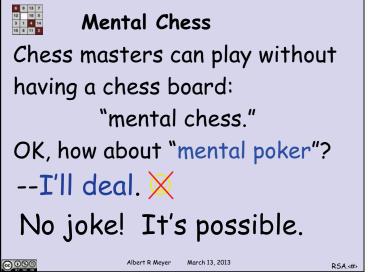
RSA.«#»

1

Albert R Meyer



RSA.«#»





000

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

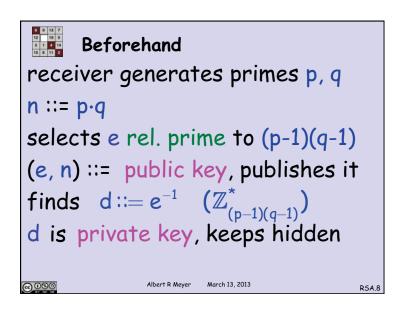
March 13 2013

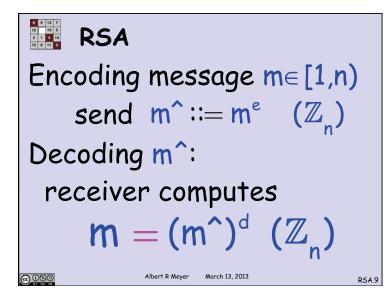
RSA.«#»

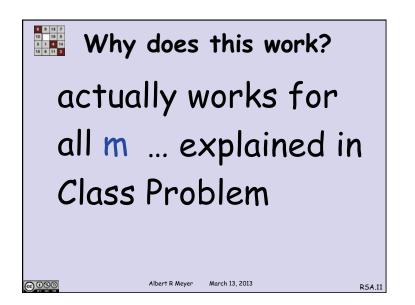
Albert R Meyer

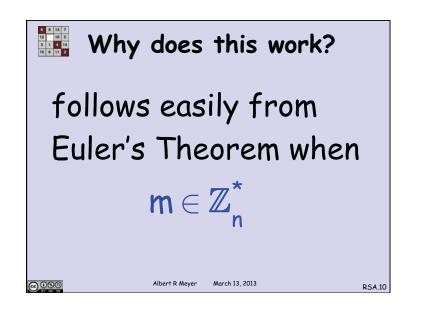


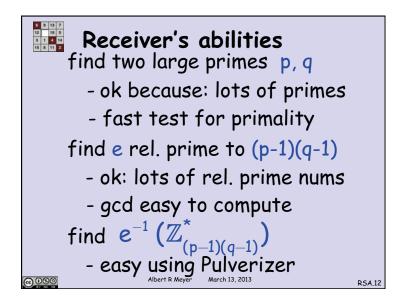


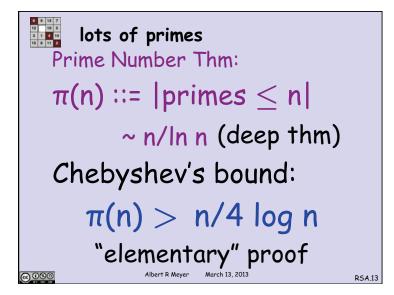








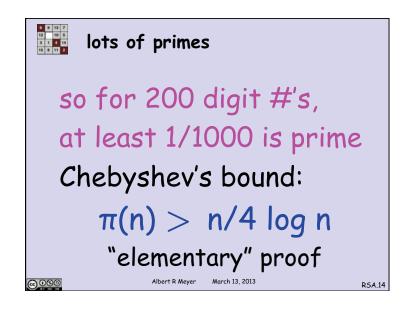


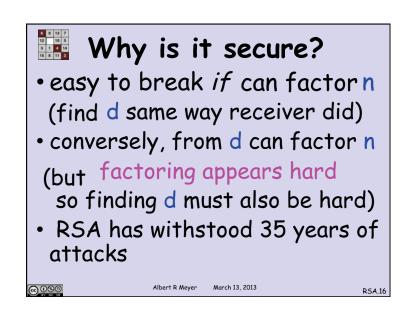


Fermat Primality Test check if $a^{n-1} = 1$ (\mathbb{Z}_n) if fails, not prime (Fermat) choose random a in [1,n). if not prime, Pr(fails)>1/2 (with rare exceptions)

Albert R Meyer March 13, 2013

RSA 15





6.042J / 18.062J Mathematics for Computer Science Spring 2015

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.