

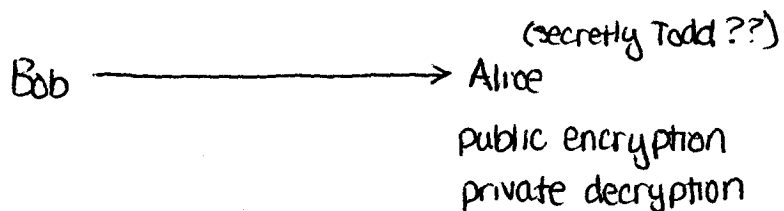
Cosca01 ~ 11/14/2011

RSA (Rivest, Shamir, Adleman ~ 1978)

↳ basis of all modern computer-based encryptions

- Note: was originally developed by UK intelligence in 1973
but was kept secret

- public key encryption



#1 concern: Alice is really Alice

Four problems you must be able to do in order
to do RSA:

① Modular Exponentiation

$$x^n \pmod{p}$$

② Greatest Common Divisor

③ Multiplicative Inverse

$$Ax \equiv 1 \pmod{p} ; \text{ given } A \text{ and } p \sim \text{solve for } x$$

④ Primality

is n prime?