Cosc201 ~ 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

Bob ⟶ Alice (secretly Todd??)

public encryption
private decryption

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

④ Primality
is n prime?