Lecture 12: Non-secret Key Cryptosystems (How Euclid, Fermat and Euler Created E-Commerce)

> Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers.
>
> G. H. Hardy, *The Mathematician's Apology,* 1940.

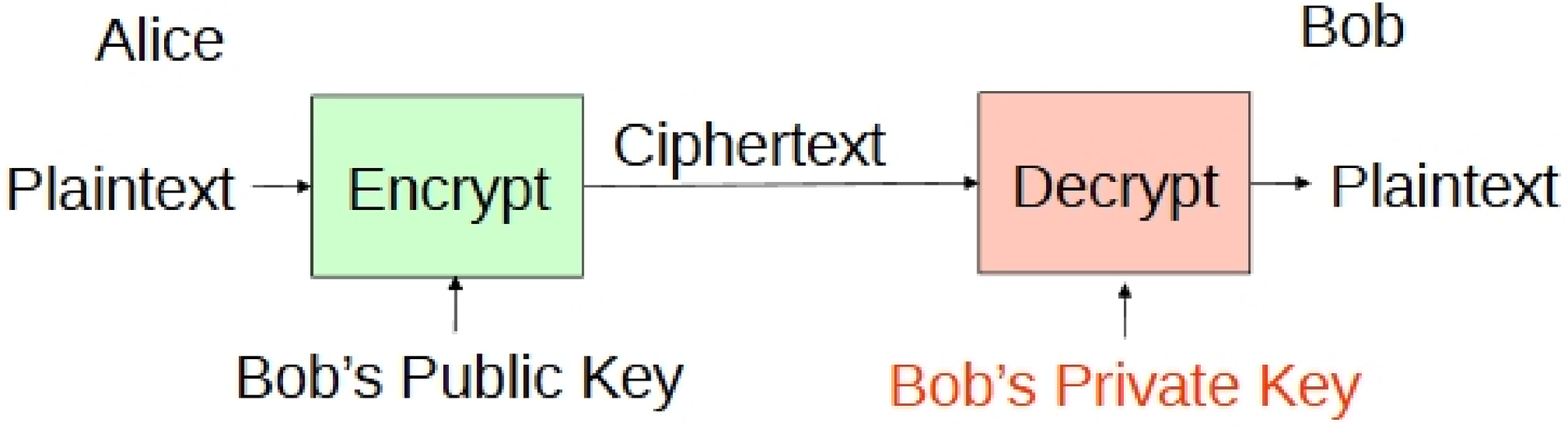
CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/evans

Applications of RSA

- Privacy:
  - Bob encrypts message to Alice using E_A
  - Only Alice knows D_A
- Signatures:
  - Alice encrypts a message to Alice using D_A
  - Bob decrypts using E_A
  - Knows it was from Alice, since only Alice knows D_A
- Things you use every day: ssh, SSL, DNS, ...

Public-Key Applications: Privacy



- Alice encrypts message to Bob using Bob's Private Key
- Only Bob knows Bob's Private Key ⇒ only Bob can decrypt message