Lecture 6: Key Exchange

> The era of "electronic mail" [Potter1977] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*.
>
> R. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, January 1978. (The original RSA paper.)

CS551: Security and Privacy
University of Virginia
Computer Science

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

Menu

- PS1
- RC6 Proof Challenge (Vic Ludwig)
- Key Distribution (Greg Lamm)
- Diffie-Hellman Key Agreement
- Intro to Public-Key Cryptosystems
- Return PS1

PS1

- Problem 2
  - Process more interesting than answer
- Problem 4
  - Even a “provably perfect” scheme breaks in practice
  - Bonus question:
    - any 98 agents obtain no information
    - any 99 agents can determine message
    - key data O(100 * n)