**Recitation 25 — Keys Under Doormats**

**Introduction**

- This is a policy paper, not a technical paper. How does it differ from what we normally read in this class?
- Who are the authors? What expertise are they bringing to this paper?
- What did you think the point of this paper was?
    - Notable consequence of this paper: Influenced the Obama administration to not pursue exceptional access (source)

**Escrow Keys**

- To use public-key cryptography to encrypt/decrypt: if A wants to send to B, A encrypts with B's public key, and B can decrypt with its secret key.
- Common use case: use public-key cryptography to exchange a symmetric key, and then encrypt data with the symmetric key.
- Escrow keys: encrypt the symmetric key twice: once with the public key of the recipient, once with an escrow agent's public key.

**Discussion**

- "Complexity is the enemy of security" — why? Can you give examples from lecture?
- The paper mentions three problems with escrow keys. The third is, who should control escrowed keys? Who *should* control them? How do we handle the fact that the Internet is global?
- "How can the technical design of an exceptional access system prevent mass surveillance that would covertly violate the human rights of entire populations, while still allowing covert targeted surveillance of small numbers of suspects?"
- "Would anonymous communications, widely recognized as vital to democratic societies, be allowed?"
- The paper (page 73, top left) references "the social infrastructure needed to support secure governmental systems." What do they mean by that?