Introduction to Modern Cryptography

9th lecture:

Public-Key Encryption

El Gamal Encryption

last time:

- Private-Key Management
- Public-Key Revolution

9th lecture (today):

- Public-Key Encryption
- El Gamal

- algorithmic number theory
- key distribution, Diffie-Hellmann
- RSA

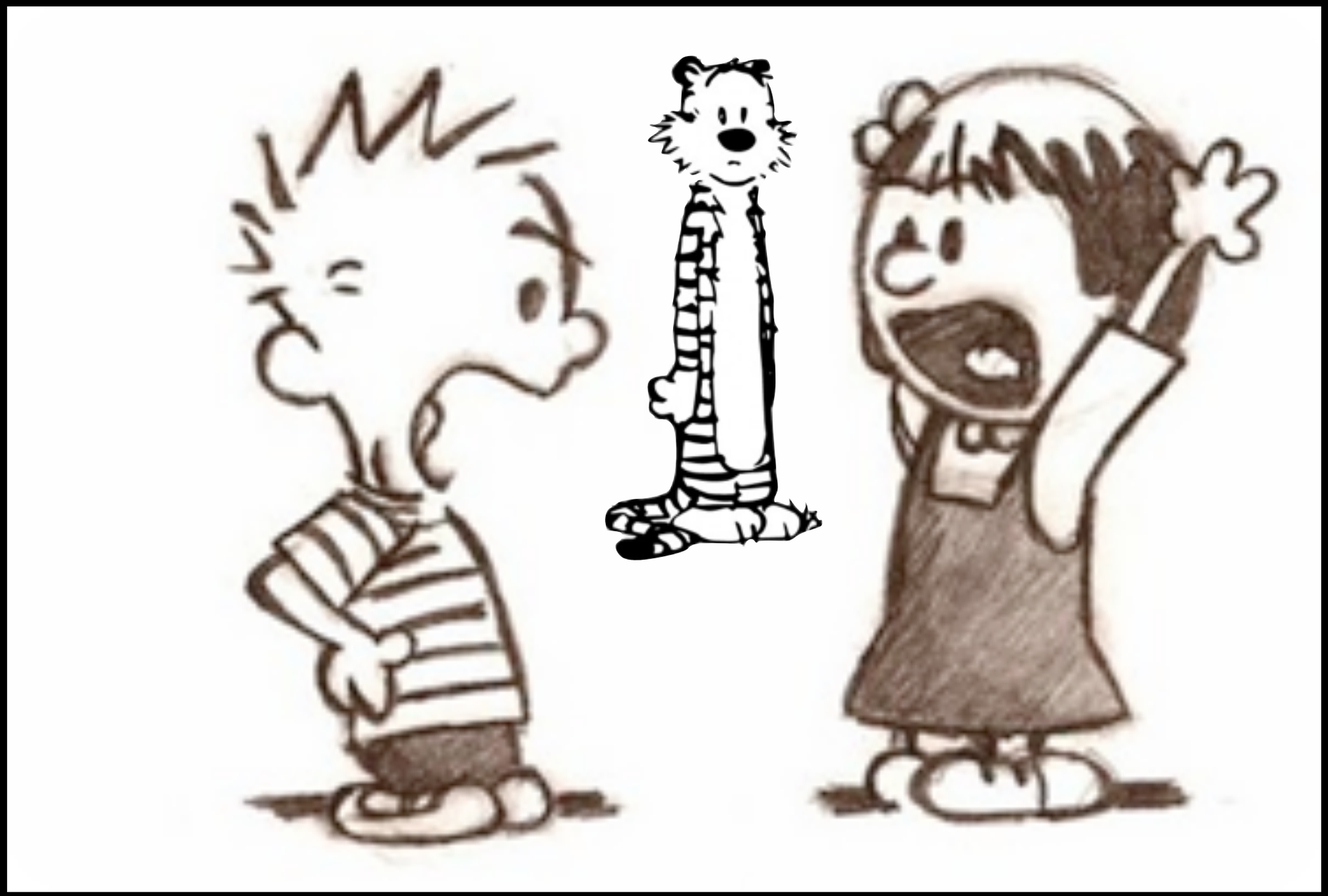
	secret key	public key
confidentiality	private-key encryption	public-key encryption
authentication	message authentication codes (MAC)	digital signatures

last time:

- Private-Key Management
- Public-Key Revolution

9th lecture (today):

- Public-Key Encryption
- El Gamal



Taher Elgamal

*1955

- 1977: BSc from Cairo university
- 1984: PhD from Stanford
- 1996: "Father of SSL" as Chief Scientist of Netscape
- CTO of various companies

- fun fact: "I read number theory books for fun!"

Recent Software Bugs

- Feb 2014: #gotofail in Apple software
- April 2014: Heartbleed in OpenSSL library, see XKCD

- 24 Sep 2014: Shellshock in Unix Bash shell

Bottom line: implementing security-related software is difficult