Centre for Information Security and Cryptography

http://cisac.math.ucalgary.ca/

"Private Parts. Man's fruitless quest, throughout history, for a means of protecting privacy."

H.C. Williams
iCORE Chair Algorithmic Number Theory & Cryptography
Department of Mathematics and Statistics
University of Calgary

UNIVERSITY OF CALGARY
FACULTY OF SCIENCE

Dimensions of privacy

- Privacy of the body (our private parts, perhaps, sometimes posted on the internet)
- Privacy of the home (Telemarketing, other intrusions like break and enter, security)
- Privacy from surveillance (CCTV everywhere these days)
- Privacy from eavesdropping (wireless devices)
- Information privacy

Private Parts

- Address, Date of Birth
- Social Insurance Number/Social Security Number
- Mother's maiden name

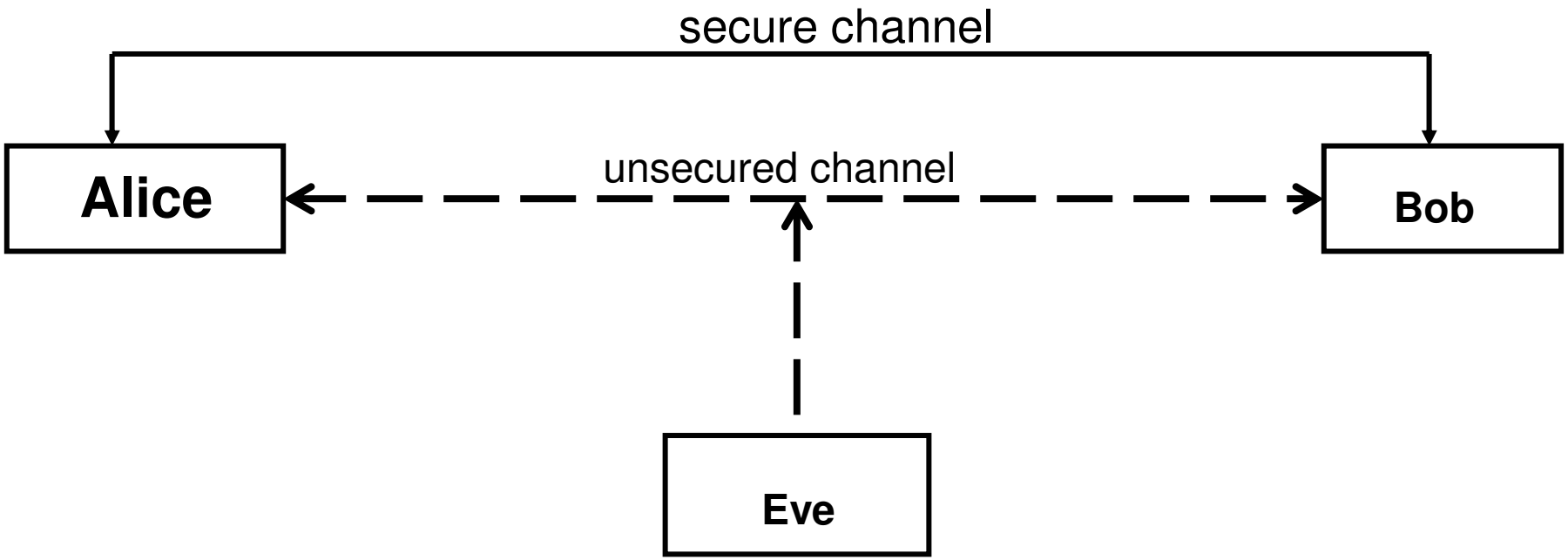
Cost of Identity Theft

- 2002 → Canada Total loss $8,829,378.45
- 2002 → Alberta 635 incidents $593,599.25
- 2003 → Canada Total Loss 8,817 incidents; $14,107,864.90
- 2003 → Alberta 724 incidents$806,745.84
- Total loss in US in 2002 54 million dollars!!!

http://www.calgarypolice.ca/ (crime prevention button)

Cryptography

- Communicating parties a priori share secret information called the key



Poe's Comment

"Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation.

Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."

- Edgar Allan Poe (1840)

Monument to Cryptanalysts

Services provided by two-key cryptography.

- **Confidentiality:** keeping data secret from all but those authorized to see it.
- **Data Integrity:** Assuring that data has not been altered by unauthorized means.
- **Data-origin authentication:** Corroborating the source of data.
- **Entity authentication:** Corroborating the identity of an entity.
- **Non-repudiation:** Preventing an entity from denying previous commitments or actions.

Security Hierarchy

- User
- Administration
- H/W, S/W Implementation
- Protocol
- Cryptographic Tool

Conclusion

"We have met the enemy and he is us."

- Walter Crawford Kelly (1913-73)