Introduction to Cryptography

Murat Kantarcioglu
What is this course about?

- We will discuss cryptographic primitives to enable
  - Data Confidentiality (only people who knows certain secret can read the confidential data)
  - Data Integrity (data is not modified without being detected)
  - Authentication (Only the authenticated people can send/receive messages in communication.)
Cryptographic Primitives

- We will *discuss* the following *primitives* in this course
  - Symmetric Encryption
  - Message Authentication
  - Public Key Cryptography
  - Digital Signatures
  - Pseudo-random Number Generators
Why Cryptography is Important?

• More than ever “Knowledge is Power”
• Cryptography provides important tools to protect important “knowledge”
  – Though cryptography is not a panacea.
• Remember the History!
  – Breaking Japanese naval code in the Battle of Midway in the second world war.
  – Breaking Enigma
  – Breaking DVD Encryption
• Watch the following clip 😊
  – http://www.youtube.com/watch?v=360vFPX-T_g
Required Background

• Cryptography is based on beautiful math
• All the required math will be taught during the class
• BUT, if you do not like to see math (e.g. proofs, equations etc.) This course may not be for you.
• In other words, mathematical maturity is needed!!!
Administrative Issues

• Check the course web site to download slides
  – [http://www.utdallas.edu/~muratk/crypto07.htm](http://www.utdallas.edu/~muratk/crypto07.htm)
• Syllabus is available on the course web site.
• Grading
  – Homeworks %20 (5 homeworks, each worth 4%)
  – Project %25 (Group project (up to 3 people) that requires programming)
  – Midterm %25 (Take home midterm)
  – Final %30
  – Class Part. %5 (Bonus for Class Participation)