Math 3CY3
Welcome back!

Bradd Hart

Sept. 5, 2018

The basics

- I am Bradd Hart and we meeting in HH 109 at 1:30 MWTh.
- The text for the course is ”Introduction to Cryptography with Coding Theory,” 2nd ed. by Trappe and Washington.
- All information about the course can be found on the course website located on my homepage (not Avenue).
- There are three in-class tests: **Oct. 4, Nov. 1 and Nov. 28**
- Assignments roughly every two weeks.
- The marking scheme for the course is

	Option 1	Option 2
Assignments	10%	10%
Tests	15% each	30%; best 2 out of three
Final	45%	60%

What is cryptography?

- A(lice) wants to communicate with B(ob).
- Classically, they might talk, write to each other, signal to each other.
- For most of history, the issue of security of this communication was restricted to military and diplomatic circles.
- Security, when it mattered, was a matter of preventing eavesdropping or interception of the communication.
- Slightly more difficult is the issue of when the communication is intentionally interrupted or replaced.

Why is cryptography? The main issues

- Security
- Privacy
- Authentication
- Errors

Codes vs. Ciphers

- Aiseray ouryay andhay!
- A cipher (formally a block cipher) is a one-to-one function from strings of characters to strings of characters.
- So given a message (string of characters) M and a cipher (function) φ, we call $\varphi(M)$ the ciphertext.
- Since φ is one-to-one, one can decipher φ with φ^{-1}.
- Is it possible to create φ that is easy to compute but φ^{-1} is hard to compute?
- Yes! More later.