Announcements on April 16

- Schedule
  - 4/16: BB Model Examples
    - Read MU 5
  - 4/18: Review for Midterm
    - **Exercises: MU chapter 5 – 2, 5, 7, 9, 10, 12, 13, 15**
  - 4/23: **Midterm**
    - You may use two A4 sized reference note, should be original, handwritten (no photo-copy), ..

Hashed Password

- Store hash values of passwords

Ann	Ann Tylor	0010111001…01
Beeth	Beth Smith	1110101000…00
Cheese	Mike Chenny	0101100010…01

Store real password database off-line (Or no database)

- Receiving a password from a user, compute its hash value using the same hash function & key
- True passwords always pass the test
  - Prob. of False negative = 0
- Sometimes, wrong passwords pass the test
- What is the prob. that a wrong password is accepted?

= Prob. that the wrong password has the same hash value

= $1/2^{256}$