Lecture 10
How Bob send Alice an engage ring
Security and mathematics

Secure mail quiz

- Bob want to send engage ring to Alice. But they live far away, and he need to mail it. Unfortunately, in their country “Kopernica”, mail is always stolen unless it is in a box locked by a padlock.
- Each of Bob and Alice has many padlocks, but has no key for padlocks of each other.
- How Bob safely send the ring (or a pair of his padlock and key) to Alice??

Deffie-Helman system

- Whitfield Deffie was captured the idea of the secure key exchange
  - He want to turn the Alice-Bob puzzle to the secure network protocol
- Martin Helman joined him, and find a way by using elementary number theory.
  - Deffie was a kind of hippy researcher and Helman was a professor of Stanford

Secure mail quiz: A solution

- Bob send the ring in a box with his padlock
- Alice receive it, set her padlock too, and send back to Bob
- Bob unlock his padlock and send back to Alice
- Alice unlock her padlock. Smile!

Easy (if once shown), but very inspiring.

Use Caeser method?

- Apply key exchange
- Alice want to send M =“ILOVEYOU”
- Her key is “14312431” ,and send A=“JORWGCRV” to Bob
- Bob use his key “21121141” and send B=“LPSYHDVW” to Alice
- Alice unlock her key by “-1,-4,-3,-1,-2,-4,-3,-1” to send C= “KMPXFZSW” to Bob
- Bob unlock is key to have D=“ILOVEYOU”.
- Smile?? What is wrong??.

Breaking the protocol

- Takeshi knows A, B, and C
- k and k’ are keys of Alice and Bob
- A = M ★ k, （★: component-wise summation)
- B = A ★k’ = M ★k★ k’
- C= B ★ (-k) = M ★ k’
- Takeshi can compute M = A ★C★(-B) ,breaking the protocol

Mathematics

- God blessed Deffie and Helman
  - Never give up, then god will help you.
- Mod p computation for a “large prime” p
- We use the following facts (proofs later):
  - Given an n bit number x and a number g < p, we can compute g^x mod p efficiently in O(n) time.
  - Given an n bit number x , we can compute x’ such that $g^{xx'} = g$ mod p efficiently.
  - But, given g and h, it is difficult to find z such that $h=g^z$
- How to use it??

Bob send M="I Love You"

- Alice and Bob agrees a prime number p
  - p is known in public, and it is larger than 2^{500}
  - The message M is a k-bite number < p
- Alice and Bob has keys x and y, respectively.
  - Both are private.
- Protocol
  - Alice sends $A = M^{x}$ to Bob
  - Bob reply $B = A^{y}$ to Alice
  - Alice compute $C = C^{x'}$ and send it to Bob
  - Bob compute $D = C^{y'}$, which is indeed M
- Takeshi knows A,B, and C but cannot compute M….

Algorithmic problems we assumed

- How to compute a large power (mod p)
  - Homework!
- How to find inverse mod p?
  - Euclid's algorithm for largest common divisor
- How to find a large prime number?
  - Prime number theorem: distribution of random numbers
  - Primarity check