CIS 5371 Cryptography

1. Introduction

A simple communication game

(Textbook: *Modern Cryptography, Theory & Practice*. Wembo Mao, Prentice-Hall, 2004.

Coin-flipping over the phone - a simple example

- Discuss the effectiveness & practicality of crypto.
- Discuss the foundations of crypto.
- Establish a mindset for developing crypto systems for Information Assurance.

Coin-flipping over the phone

Alice and Bob have just split up.

They now live in different towns and must decide who will get take their 1967 Stingray Corvette.

They decide to flip a coin over the phone.

Alice doesn't trust Bob:

So she must:

1. (*Hiding property*: *Bob should not be able to cheat*) Hide her choice from Bob, but also
2. (*Binding property*: *Alice should not be able to cheat*) Commit to her choice,

Coin-flipping over the phone

Bit Commitment function f

- f is an integer function
- f is easy to evaluate

  For any $x \in I$ it is easy to compute $f(x)$
- Hiding property

  Given $f(x)$ it is hard to find x.
- Binding property

  It is hard to find any other integer y such that $f(y) = f(x)$.

Coin-flipping over the phone

Coin-flipping protocol

Alice and Bob agree on a commitment function f, and that if Bob can guess correctly the parity of a number x that Alice will select then he wins (gets the Corvette).

1. Alice selects a *large* random number x and computes $f(x)$: she tells Bob the value of $f(x)$ over the phone.
2. Bob tells Alice over the phone his guess of the parity of x.
3. Alice tells Bob over the phone the value of x.
4. Bob first checks the correctness of x by evaluating $f(x)$ and then the correctness of his guess. If he x is incorrect or if he guessed correctly the parity of x, then he wins; otherwise he loses.

Coin-flipping over the phone

Security Analysis of the Coin-flipping protocol

- Since the commitment function f *hides* the value x, Bob cannot determine its parity.
- Since the commitment function f is *binding* Alice cannot choose later (after being told Bob's guess of the parity of x), a value y with different parity such that $f(y) = f(x)$ (in case Bob has guessed correctly the parity of x).
- So Bob cannot do better than guessing and Alice cannot cheat.
- This is an informal proof. The scope of this course is to develop the necessary techniques and methodologies for analyzing formally the security of cryptographic protocols.

Foundations of cryptography

- Modern crypto is based on crypto primitives such as the one just used.
- The existence of a bit commitment function implies the existence of a secure crypto system, and conversely,
- The existence of a secure crypto system implies the existence of a commitment function.

Cryptographic primitives

- *Bit commitment* is one crypto primitive.
  There are many others.
- *One-way functions* are another very important crypto primitive.
- It can be shown that
  one-way functions $\Rightarrow$ *bit-commitments*
- Other important crypto primitives are:
  - *Hash functions*
  - *Digital signatures*
  - *Encryption functions*

Criteria for desirable crypto systems

What is a good cryptographic system/protocol?

- Conceptually simple.
- Efficient in practice.
- Proven secure in some security model/framework.
- Based on well established primitives and services.

Modern role of cryptography

- Support Internet security: privacy integrity, authentication, anonymity
- Support e-commerce, e-government and other e-applications
- Support system security.