Lecture 01 (Introduction)

1 What is Course About?

1. Cool maths
2. Not cryptocurrency
3. Not computer security
4. Not blockchains

2 Course Contents

1. Foundations of real world digital systems
2. Formal security definitons and security proofs
3. Theoretical course

3 Objectives

1. Develop 'crypto mindset'
2. Modelling threats via security definitions
3. Learn the 'atomic' building blocks of crypto
4. Understand how to prove security

4 4-Step Recipe for a Crypto Primitive

1. Define security for primitive
2. Figure out required building blocks
3. Propose construction
4. Prove construction satisfies security definitions

(any) Theorem: Assuming building blocks $\exists$ construction satisfying the definition

Issue with this:

1. Building block itself could be broken
2. Security definition might be incomplete

4.1 Building blocks are analogous with lego blocks :)

1. Blocks are immutable ≡ DO NOT modify building blocks
2. Can't manufacture blocks ≡ DO NOT implement building blocks

5 Why Formal Definitions?

5.1 Symmetric Key Encryption

Key space: $\mathbb{K}$

$$encrypt(message, key) \rightarrow ciphertext$$

$$decrypt(ciphertext, key) \rightarrow message|\perp$$

Correctness: $decrypt(encrypt(m, k), k) == m$

5.2 What Needs to be Ensured?

1. Adversary should not be able to learn any part of m
2. (??) Probability distribution does not change

5.3 Messed Up Ciphers in History

1. Caesar's cipher - brute force
2. Substitution cipher - frequency analysis
3. Vigenere's cipher - brute force on n + substitution cipher algo
   i. secret key = n different permutations
   ii. encryption = encode i^{th} character with $i \mod n^{th}$ permutation
   iii. Is double encrypt Vignere secure? - NO. Since it is just a new permutation
   iv. Is Vignere with $n = |m|$? - NO. Unless it is used only once
4. (rotor machines) Enigma
5. Shannon's One-Time Pad - first perfectly secure algorithm
   - key cannot be re-used
   - key must be as large as message
6. Date Encryption Standards (DES)
   i. key space = $\{0,1\}^{56}$
   ii. encrypts/decrypts 64 bit blocks at a time
   iii. 56 was chosen since US had powerful computers and they could brute-force and decode but not others
7. Double DES (2DES)
   i. key space = $\{0,1\}^{112}$
   ii. performs DES twice on 64 bit blocks
   iii. previous attakcs infeasible
   iv. a different (very simple) attack breaks 2DES (which also breaks DES)
8. Advanced Encryption Standard (AES)

i. key space = $\{0,1\}^{128}$
ii. encrypts/decrypts 128 bit blocks at a time
iii. no efficient algorithm for breaking AES

6 Building Blocks

Hard computation problems are building blocks

6.1 Sources

1. Cryptographic standards: AES, SHA, etc.
2. Number theory
3. Geometry
4. Combinatorics

#Misc We'll only see tip of iceberg of crypto

7 Crypto is Magic!

7.1 Magic 1 - Oblivious transfer

1. Bob should learn x_b (b is a bit)
2. Alice should not learn b
3. Bob should not learn x_{1-b}

7.2 Magic 2 - Multiparty computation

1. Alice and Bob should learn $f(x_0, x_1)$
2. Alice should not learn x_1
3. Bob should not learn x_0

7.3 Magic 3 - Zero Knowledge Proof

1. Convince that solutions exists
2. Don't reveal solution

8 Course Policy

1. Theoretical proofs
2. LaTeX assignments
3. Minor - 25
4. Major - 30
5. Assignments (4) - 25

6. Quizzes (best 5 of 6) - 20 (non-surprise, during class hours)
7. (?) Open-notes but handwritten only :(
8. (?) Longer duration for exams?
9. Three late days cumulative for assignments
10. Audit - 30% cumulative and 30% in exams