Techniques in Applied Cryptography

CSCE 689

Section 602

Instructor:

Yupeng Zhang, HRBB 414A

office hour by appointment, zhangyp@tamu.edu

Instructor:

Yupeng Zhang, HRBB 414A

office hour by appointment, zhangyp@tamu.edu

Time and Location:

Tuesday and Thursday 12:45-2:00pm, HRBB 126

Course Description

Applied Cryptography

- Basic concepts
- State-of-the-art constructions
- Applications
- Research directions

Topics

- Secure Multi-Party Computation (MPC)
  - Privacy-preserving Machine Learning
- Searchable Encryption
  - Search on Encrypted Files
- Zero Knowledge Proof
  - Privacy-preserving crypto-currencies and smart contract

Webpage and piazza

- https://tamucsce.github.io/csce689/
- piazza.com/tamu/fall2019/csce689section602

Date	Section	Topic
8/27	Introduction	Introduction and logistics
8/29	Secure Multiparty Computation and Privacy-Preservin g Machine Learning	Introduction to secure multiparty computation
9/3		Yao's garbled circuit
9/5		GMW protocol
9/10		Background on machine learning algorithms
9/12		Privacy-preserving machine learning
9/17	Searchable Encryption	Introduction to searchable encryption
9/19		Dynamic searchable encryption
9/24		No class due to travel
9/26		
10/1		Forward and backward security
10/3		Attacks to searchable encryption
10/8		Locality of searchable encryption

Date	Section	Topic
10/10	Verifiable Computation, Zero Knowledge Proof and Blockchain	Introduction to verifiable computation and zero knowledge proof
10/15		Customized solutions: Authenticated data structures
10/17		
10/22		Generic solutions: SNARK
10/24		
10/29		Midterm project presentation
10/31		Generic solutions: Interactive proof
11/5		
11/7		
11/12		Introduction to blockchain, crypto-currency and smart contract
11/14		Privacy-preserving crypto-currencies
11/19		Privacy-preserving smart contract
11/21	Project presentations	
11/26		
11/28		No class, Thanksgiving
12/3		

Grading Policy

- **Class participation (10%):**

- **Reading assignment (25%):**

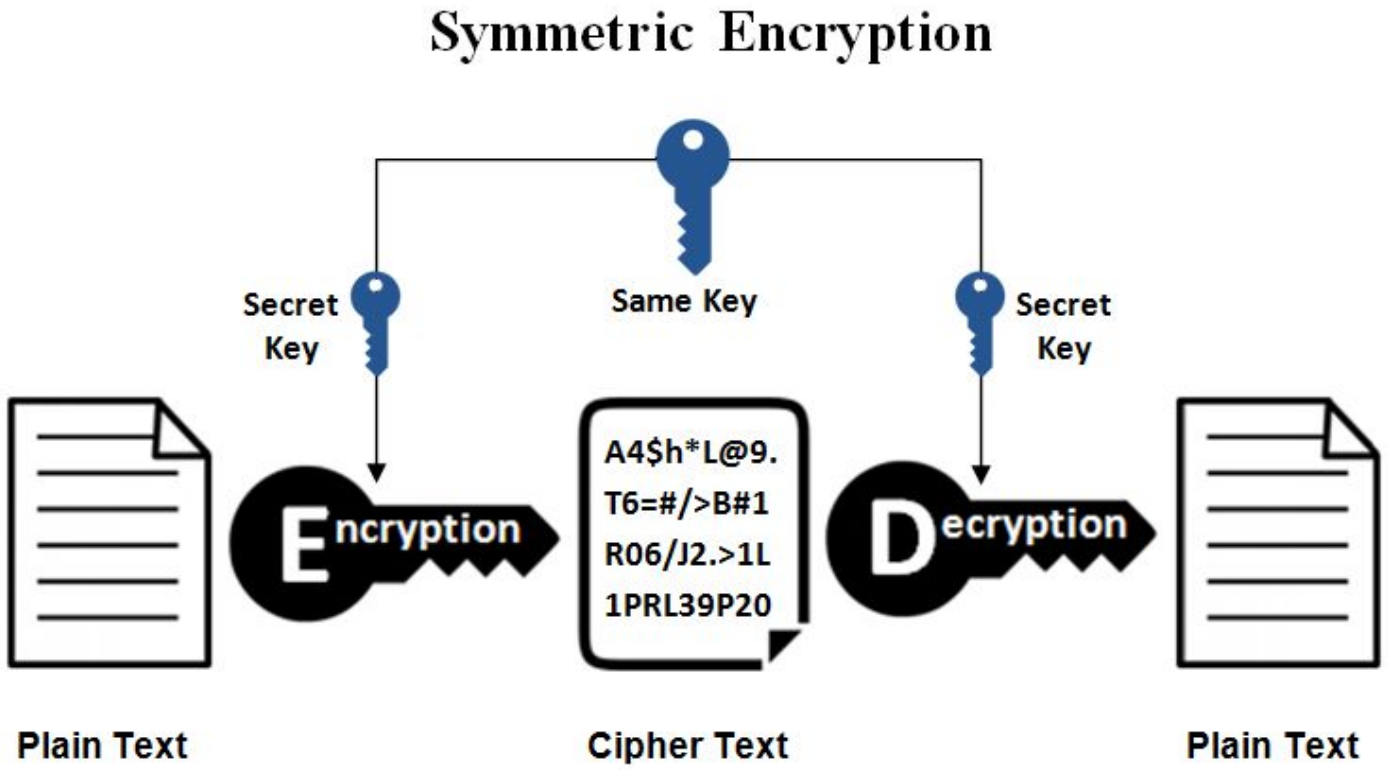
- **Project (65%):**
  - Proposal (10%)
  - Mid-term report and presentation (10%)
  - Final presentation (20%)
  - Final report (25%)

Projects

- 2-3 people each team. Team formation due 9/10.
- Post list of suggested projects later. You can come up with your own ideas.
- Discuss the projects with me before proposal. Proposal due 9/26.

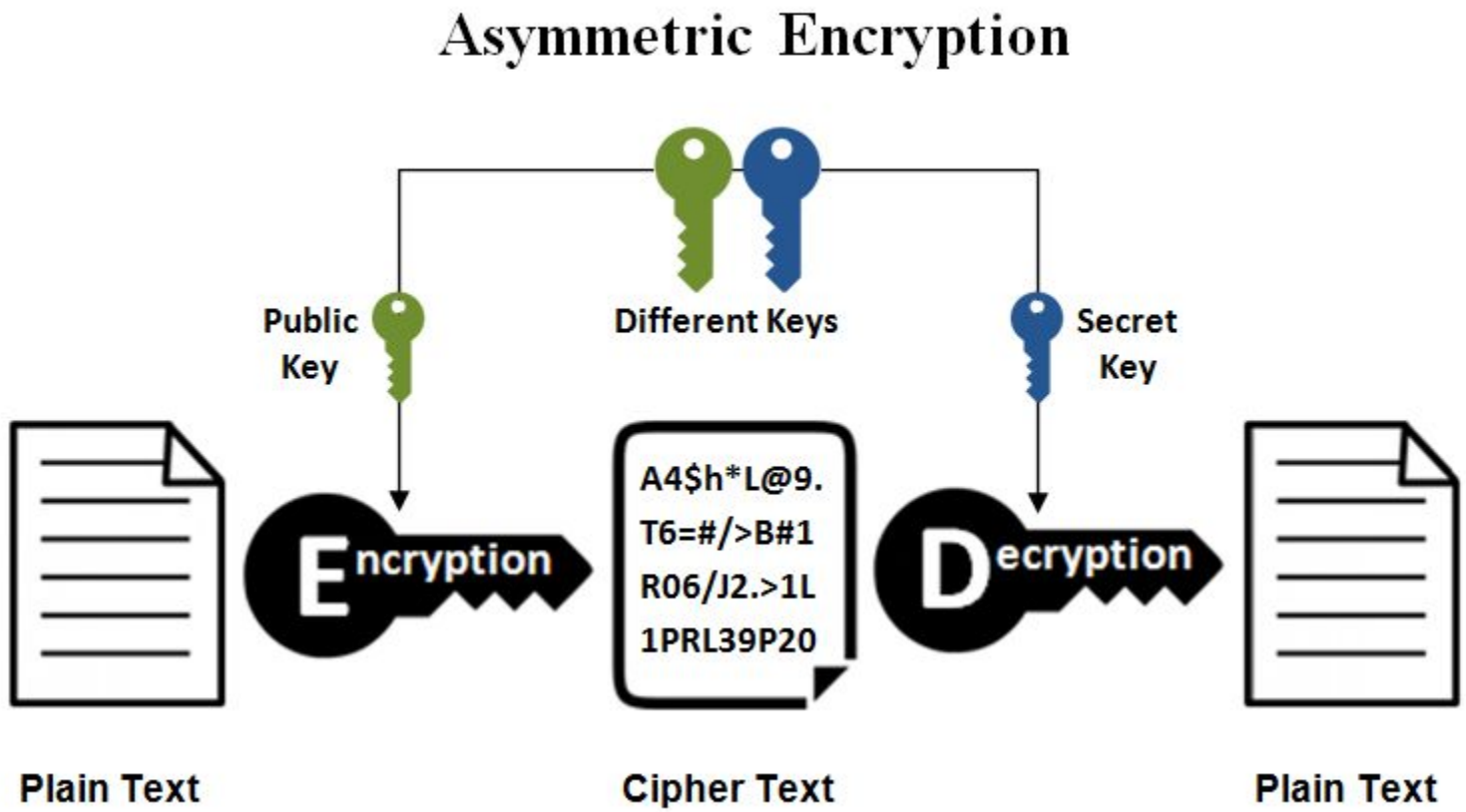
Background

Encryption



Deterministic vs. randomized

Public key encryption (Asymmetric)



Message authentication code and signatures

- Integrity
- Symmetric: message authentication code (MAC)
- Asymmetric: signature

Cryptographic hash function

- $H: \{0,1\}^* \rightarrow \{0,1\}^k$ any string to 256-bit string, deterministic

- Collision resistant: hard to find x,y such that H(x) = H(y)

- One-way: easy to compute, hard to invert
  (find x such that H(x) = y)

Algorithms, data structures and asymptotic complexity

- Binary tree, hash table, skip list etc.

- Big O notation O(n), O(2^n)

Binary representation

Boolean circuits

- AND, OR, NOT, XOR, NAND
- Truth table

Arithmetic circuits

- + and × modulo a prime p
- Universal, can simulate Boolean circuits

Field and finite field

- + and × modulo a prime p
- Generator of the group g (e.g. 2) s.t. $g^1, g^2, \ldots, g^{p-1}$ generates all elements in the group
- Discrete-log assumption: hard to compute x such that $g^x = y$