CS 4501-6501 : Topics in Cryptography

Instructor: Mohammad Mahmoody (Rice Hall 511)
mohammad@cs.virginia.edu

Time and Location: Mon Wed 10:30am-11:45am, Rice Hall 340

Office Hours: Tues 2-3:30

Credit: 3 (no 1 credit option)

What we do in a nutshell…

In this seminar we will **(mostly)** read research papers about some **(mostly)** recent developments in foundations of Cryptography. The topics will be **(partially)** chosen based on the interest of the participants, but some possible suggested topics are …

Prerequisites

Required: Discrete Math CS 2102 + Theory of Computation CS 3102

1. **Ability to read and write mathematical proofs and definitions.**

2. **Familiarity with algorithms – proving correctness and analyzing running time (O notation).**
   So CS 4102 (Algorithms) would be extremely helpful.

3. **Familiarity with basic probability theory**

Sufficient:

Complexity (Spring 2014)

Cryptography (Fall 2014)

Difference compared to Crypto Course

In Crypto course (Fall 2014) we paid attention to details to build foundation of crypto step by step.

Here we will go over more disperse topics and won't have time to go into as much details.

Many times this semester certain crypto tools and background would be necessary. Either I will discuss them in class or links to related resources would be provided.

Grading

70% Semester-long group projects.

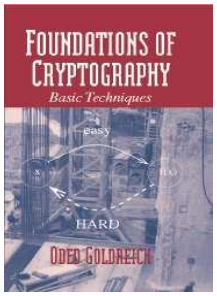
30% Class Contribution.

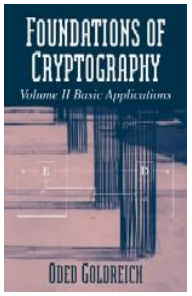
Projects: in groups of (1 or) 2 or 3

Note that more would be demanded from bigger groups, but it is not a linear function (a submodular / concave one).

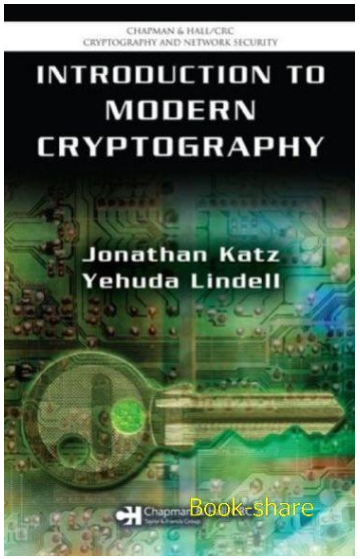
Reading

Foundations of Cryptography / Goldreich.





Introduction to Modern Cryptography: Principles and Protocols /
Kats and Lindell



Online courses (e.g. this one by Dan Boneh)
https://class.coursera.org/crypto-preview/lecture

And many papers…

What we do in more than a nutshell…

What is Cryptography

Crypto:

From Ancient Greek κρυπτός (*kruptós*, “hidden, secret”).

Almost a correct meaning for pre-modern cryptography.

Related terms:

Plain text – Ciphertext (and cipher as the method)

Cryptanalysis: study of ciphers, ciphertext, or cryptosystems (that is, to secret code systems) with a view to finding **weaknesses** in them…

Pre-modern crypto…

History of 2500- 4000 years.

Throughout most of this history:

cryptography = “secret writing”:

“Scramble” (encrypt) text

➔ **unreadable by anyone except the intended receiver that can decrypt it.**

Modern Crypto

More suitable Definition for modern crypto:

The discipline concerned with communication security (eg, confidentiality of messages, integrity of messages, sender authentication, and many other related issues), regardless of the used medium such as pencil and paper.

Related term not to be confused with:

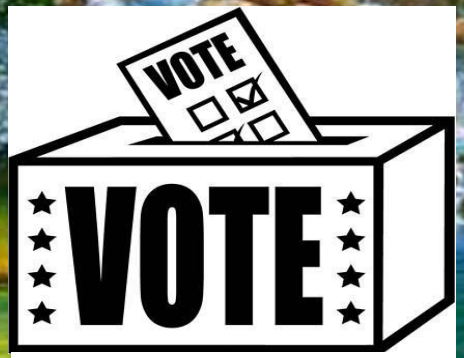
Coding: usually confused with “encryption”… an information theoretic (yet related) huge and deep area of its own…

Modern Crypto Wonderland

Secure Encryption

Electronic Auction

many more …



Electronic Voting

Contrast in Method

Recurring theme: (until 1970's)

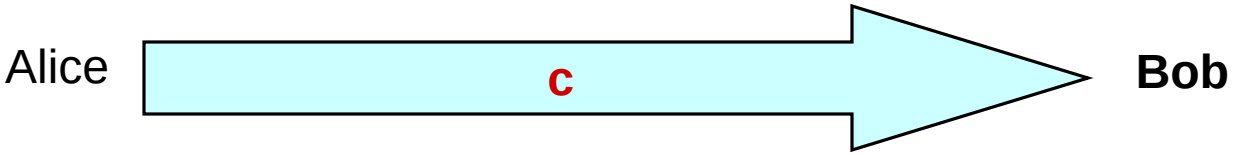
- Secret code invented
- Typically claimed "unbreakable" by inventor
- Used by spies, ambassadors, kings, generals for crucial tasks.
- Broken by enemy using **cryptanalysis**.

Modern Crypto: Pays attention to foundations and principles

- Right Definitions of "security"
- Basic "primitives" / "assumptions".
- Proofs of Security

Encryption Schemes

Alice wants to send Bob a secret message.



c = E(m,k) **m' = D(c,k)**

They agree in advance on 3 components:

- **Encryption algorithm: E**
- **Decryption algorithm: D**
- **Secret key: k**

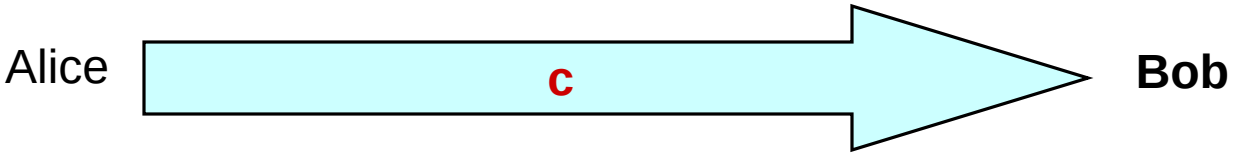
To encrypt plaintext m, Alice sends c = E(m,k) to Bob.

To decrypt a cyphertext c, Bob computes m' = D(c,k).

- **A scheme is valid if m'=m**
- **Intuitively, a scheme is secure if eavesdropper can not learn m from c.**

Review of Encryption Schemes

Alice wants to send Bob a secret message m in form of cipher c.



c = E(m,k) **m' = D(c,k)**

▪ Encryption algorithm: E ▪ Decryption algorithm: D ▪ Secret key: k	To encrypt m, Alice sends c = E(m,k) to Bob. To decrypt c, Bob computes m' = D(c,k).

Q: Can Bob send Alice the secret key over the net?

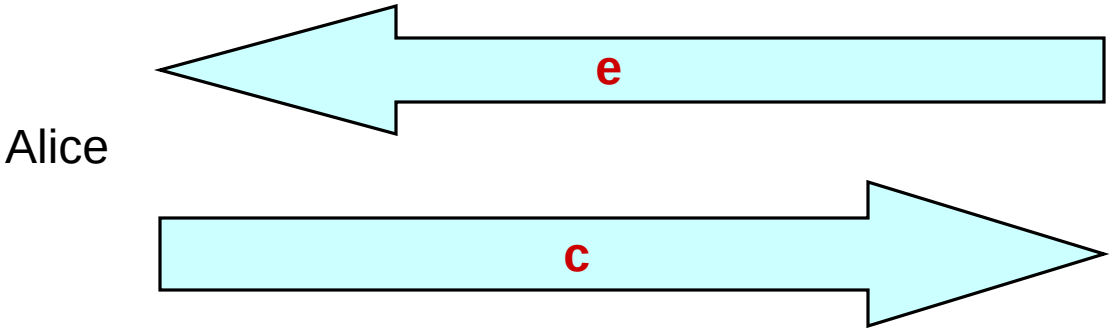
A: Of course not!! Eve could decrypt c!

Q: What if Bob could send Alice a "crippled key"

useful only for encryption but no help for decryption

Public Key Cryptography [DH76,RSA77]

Alice wants to send Bob a secret message.



c = E(m,e)

choose d,e
m' = D(c,d)

- **Encryption algorithm: E**
- **Decryption algorithm: D**
- **Key: Bob chooses two keys:** **Secret key d for decrypting messages.**
  Public key e for encrypting messages.

To encrypt m, Alice sends c

Should be safe to send e "in the cloud"!

Even if Eve knows the key e!

- **A scheme is valid if m'=m**
- **Intuitively, a scheme is secure if eavesdropper can not learn m from c.**

Other Crypto Wonders

Digital Signatures. Electronically sign documents in unforgeable way.

Zero-knowledge proofs. Alice proves to Bob that she earns <$50K without Bob learning her income.

Privacy-preserving data mining. Bob holds DB. Alice gets answer to one query, without Bob knowing what she asked.

Playing poker over the net. Alice, Bob, Carol and David can play poker over the net without trusting each other or any central server.

Secret Sharing. Distribute sensitive data to 7 servers such that any 3 of them learn nothing but any 4 can find out everything.

More Recent Crypto Wonders

Computation on Hidden Data. Also known as fully-homomorphic encryption. A server holds encrypted data over which it can do almost any computation ***while encrypted.***

Delegation of Computation. Server does the computation for you, but you don't have to trust the server, it will provide a proof as well…

Efficient Secure Computation. New methods for multi party secure computation with more efficiency (under stronger assumptions).

Universal Composability. Run protocols concurrently over the Internet without compromising their security.