CS 442
Introduction to Cryptography

Lecture 1: Introduction

Instructor: Aarushi Goel
Spring 2026

What is Cryptography?

- Old Oxford dictionary definition:

  the art of writing and solving codes

- Modern cryptography:

→ the study of mathematical techniques for securing digital information, systems and distributed computations in untrusted environments.

→ Helps control access to information:

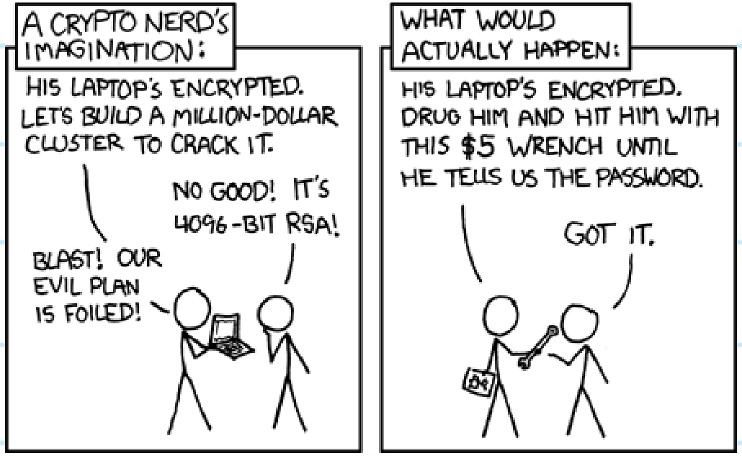
  * "who" learns "what" * "who" can influence

→ Forms the backbone of modern digital security.

What Cryptography Cannot Protect from.

* When you use it: It does not solve all security problems

→ social engineering attacks (phishing attacks, trusting the wrong person)



* When you implement it: Reliable only when implemented & used correctly

* When you build cryptosystems: Rely on well-studied standard primitives instead of inventing your own designs and assumptions.

Cryptography is used Everywhere !!

* Secure Communication

→ web traffic : HTTPS

→ wireless traffic : 802.11i WPA2 (& WEP), GSM, bluetooth

→ Whatsapp, Signal, Proton mail

* File and Disk Encryption

EFS, TrueCrypt, LUKS

* Content Protection (e.g. DVD, Blu-rays)

CSS, AACS

Size	510 GB (5,10,10,91,55,328 bytes)
Contents	LUKS Encryption (version 2) — Unlocked

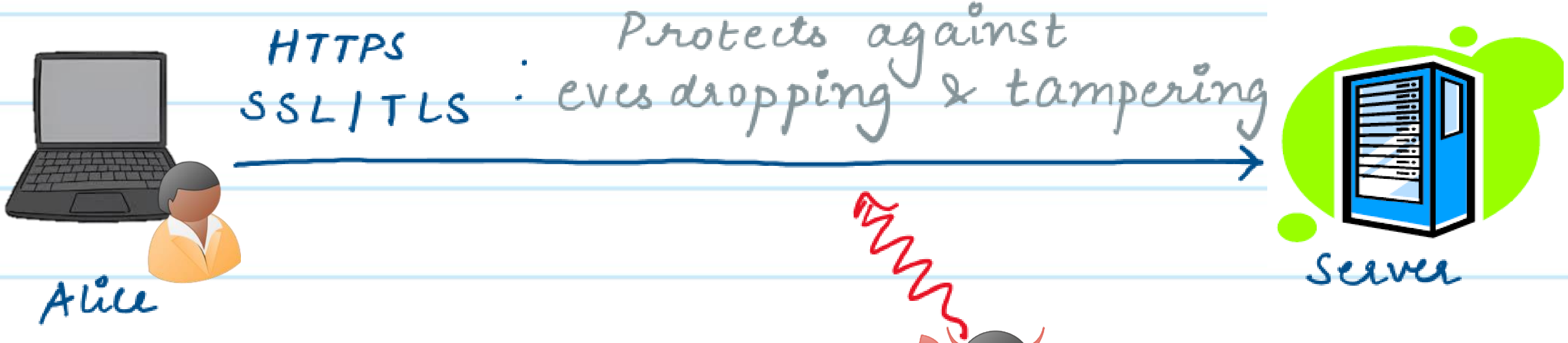
* User Authentication

→ password hashing
→ multi-factor authentication
→ biometric authentication
→ FIDO/ WebAuthn etc

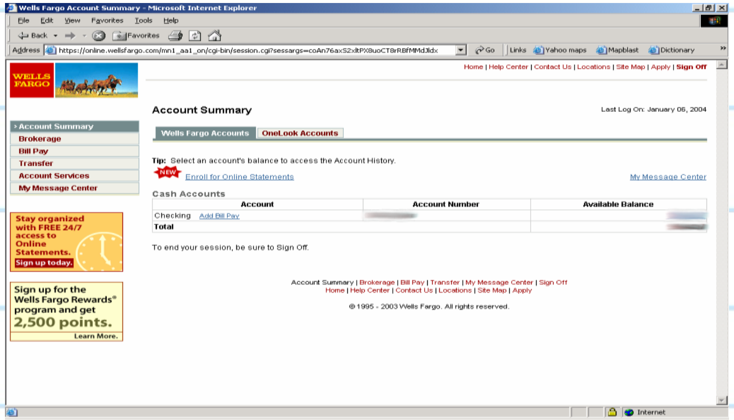
* Finance

→ Swift
→ Cryptocurrencies
→ Credit / Debit Cards

Secure Communication



HTTPS
SSL/TLS : Protects against eves dropping & tampering



Account Summary

Last Log On: January 06, 2004

Tip: Select an account's balance to access the Account History.

Enroll for Online Statements

My Message Center

Cash Accounts

Account	Account Number	Available Balance
Checking Add Bill Pay	[redacted]	[redacted]
Total		[redacted]

To end your session, be sure to Sign Off.

Stay organized with FREE 24/7 access to Online Statements. Sign up today.

Sign up for the Wells Fargo Rewards® program and get 2,500 points. Learn More.

Account Summary | Brokerage | Bill Pay | Transfer | My Message Center | Sign Off
Home | Help Center | Contact Us | Locations | Site Map | Apply

© 1995 - 2003 Wells Fargo. All rights reserved.

Secure Communication

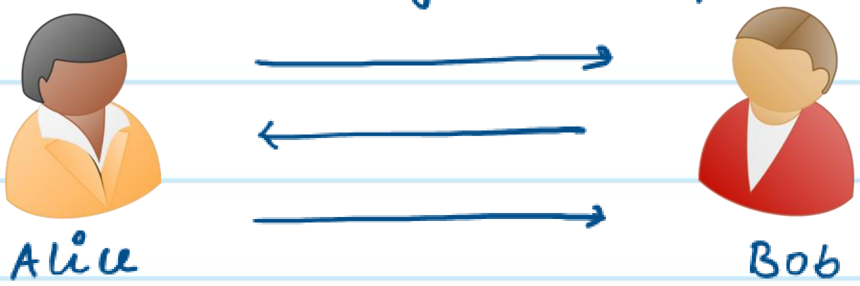
Two-main components of SSL/TLS:

* Handshake Protocol: establish a *shared secret-key* using public-key cryptography.

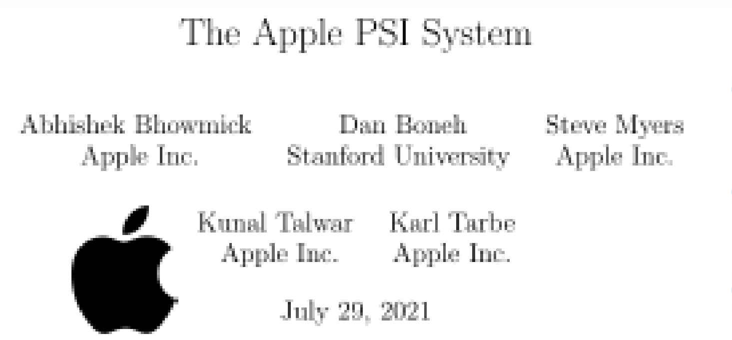
* Record Layer: Send data securely (ensuring confidentiality and integrity) using the *shared secret key*.

Private Set Intersection

Alice & Bob want to compute an intersection of their private sets



Security: Alice (resp. Bob) should not learn any information about Bob's (resp. Alice's) set, except the intersection.



The Apple PSI System

Abhishek Bhowmick
Apple Inc.

Dan Boneh
Stanford University

Steve Myers
Apple Inc.

Kunal Talwar
Apple Inc.

Karl Tarbe
Apple Inc.

July 29, 2021

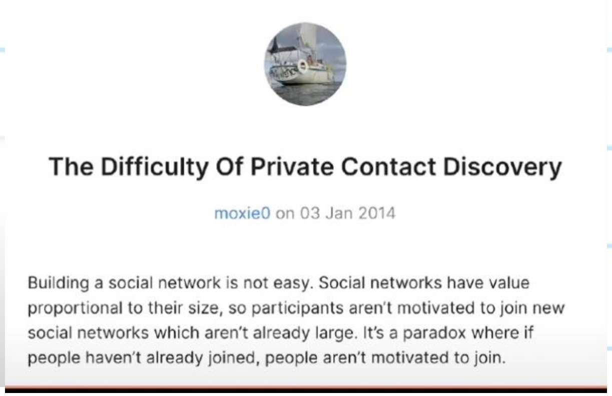
Google

Password Checkup extension

Offered by: google.com

★★★★☆ 295 | Productivity | 900,000+ users

By Google



The Difficulty Of Private Contact Discovery

moxie0 on 03 Jan 2014

Building a social network is not easy. Social networks have value proportional to their size, so participants aren't motivated to join new social networks which aren't already large. It's a paradox where if people haven't already joined, people aren't motivated to join.

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN IN SUBSCRIBE

LILY HAY NEWMAN SECURITY 06.19.2019 09:00 AM

Google Turns to Retro Cryptography to Keep Data Sets Private

Google's Private Join and Compute will let companies compare notes without divulging sensitive information.

Tentative Plan for this Course

* Secure Communication in Shared-Key Setting

→ Symmetric key encryption

→ Message authentication

→ Cryptographic hash functions

* Secure communication in public-key setting

→ Public key encryption

→ Digital Signatures

* Advanced Primitives

→ Zero-Knowledge Proofs

→ Secure Multiparty computation

→ More .... (time permitting)

Course Objectives

* Learn about the core primitives used in the design of modern cryptosystems

* Analyze the security properties required for these primitives

* Learn how to formally define them.

* Learn constructions of these primitives

* Learn how to write security proofs.

Learn the modern, provable security based approach to Cryptography.

Pre- Requisites

- * Discrete maths is required
- * Familiarity with :
  - → basic probability theory
  - → computational complexity
  - → mathematical proof techniques

No background in cryptography is necessary.

Basic Information

- Course Website: https://aarushigoel.github.io/courses/Spring%202026/CS442.html
- Office Hours: Thursdays 3:30-4:30pm, Hill 418
- Ed Discussion: https://piazza.com/rutgers/spring2026/cs442
- Homework submission via Gradescope (on canvas)

- TA: Yuange Li
- email: yl1407@rutgers.edu
- Office Hours:

Grading Policy

10%	Class Participation
30%	Midterm Exam
40%	Final Exam
20%	Homeworks (best 5 out of 6)

Late Submission : Up to 24 hrs late (50% penalty)

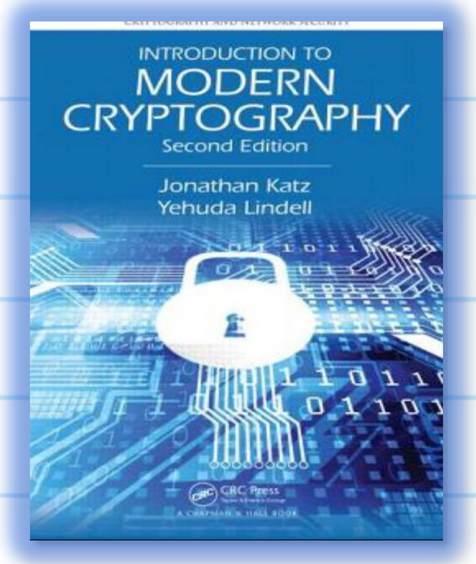
Collaboration Policy for Homeworks

* can collaborate with your classmates, but the final write-up should be your own. Mention names of everyone with whom you collaborate

* can refer to books or online resources listed on the course website. DO NOT copy anything verbatim. Acknowledge all resources that you refer to

* DO NOT use any AI tools.

Books

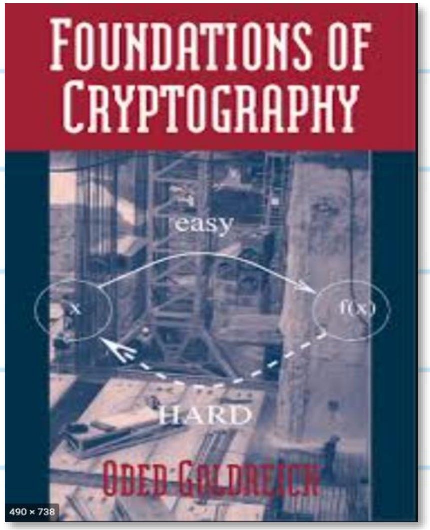


INTRODUCTION TO
MODERN
CRYPTOGRAPHY
Second Edition

Jonathan Katz
Yehuda Lindell

A Graduate Course in Applied Cryptography

Dan Boneh
Victor Shoup



FOUNDATIONS OF CRYPTOGRAPHY

ODED GOLDREICH

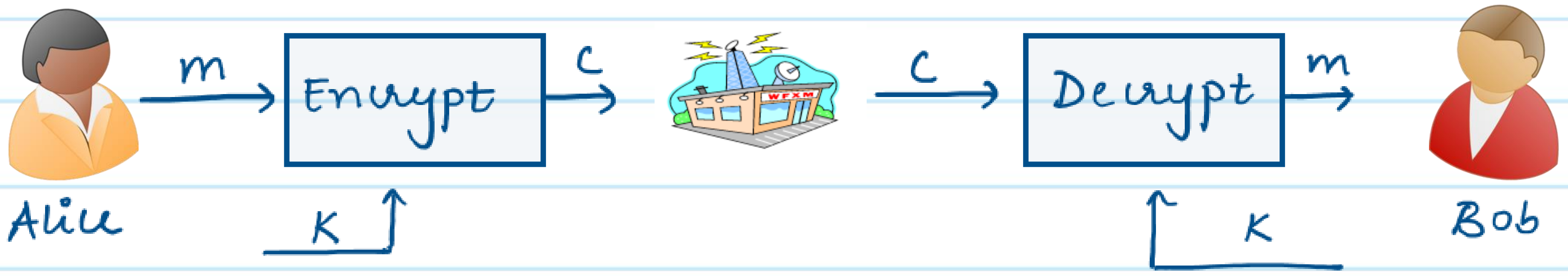
Joy of Cryptography

Mike Rosulek

Other useful resources on the course website.

Some Historic Ciphers

Symmetric-Key Encryption



m: plaintext message (comes from some space $\mathcal{M}$)

c: ciphertext (hidden) message. (comes from space $\mathcal{C}$)

k: shared common key (comes from some space $\mathcal{K}$)

Kerckhoff's Priciple

- * The cipher method must not be required to be a secret, and it must be able to fall into the hands of the enemy without any inconvenience.
- * Security should only rely on the secrecy of the key.

Auguste Kerckhoffs
19th-century
Dutch cryptographer

Kerckhoffs is right because...

* Maintaining Privacy of a short key (≈100 bits) is easier than maintaining privacy of a large algorithm.

* Easy to replace the key than a whole program if exposed.

* It is infeasible to imagine a secret pair of algorithms for every pair of communicating parties

Kerckhoffs is right because...

More reasons to have an open cryptographic design:

- Open designs undergo public scrutiny, and hence, are likely to be stronger
- Security flaws (if they exist) can be revealed by ethical hackers.
- Public designs enable establishment of standards.

Dangerous to use proprietary Encryption schemes!

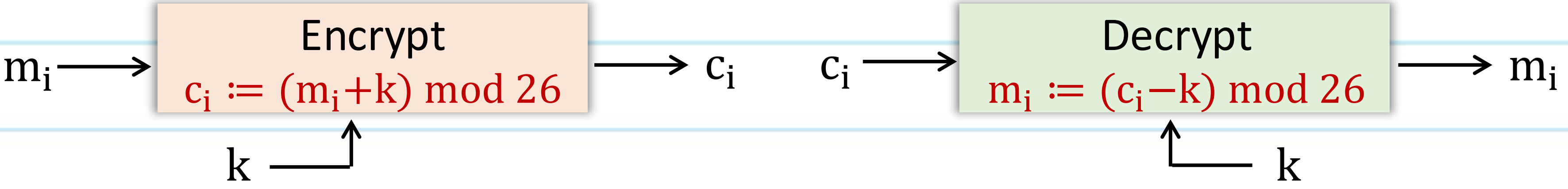
Shift Cipher (~58 BC)

Key space: $\mathcal{K}=\{0,1,\ldots,25\}$. Choose key $k\in\mathcal{K}$ at random

Encryption Algorithm: Shift by k.

Example: $k=3$

msg	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C



! BROKEN ! : Brute-force attack. Try all 26 keys.

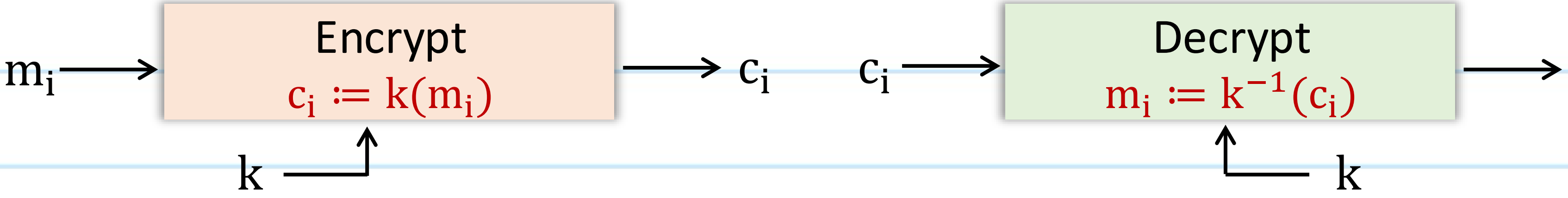
Mono-alphabetic Subsitution cipher (1300s)

Key Space: $\mathcal{K}$ = all permutations on $\{0, 1, \ldots, 25\}$. Choose k at random from $\mathcal{K}$.

Encryption Algorithm: Shift using map k.

msg	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
cipher	c	a	z	y	w	g	b	d	j	o	q	n	e	f	r	s	v	t	u	i	h	m	v	p	k	l

k: Secret mapping



Encrypt

$c_i := k(m_i)$

Decrypt

$m_i := k^{-1}(c_i)$

$|\mathcal{K}| = 26! = 2^{88}$. So no brute force attack is feasible.

Mono-alphabetic Subsitution cipher (1300s)

! Still BROKEN ! Frequency / statistical Analysis.

(exploiting statistical patterns in english language)

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWN
CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVF
ZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	**36**	→ E
N	**34**	
U	**33**	→ T
P	**32**	→ A
C	**26**	

NC	**11**	→ IN
PU	**10**	→ AT
UB	**10**	
UN	**9**	

digrams

UKB	**6**	→ THE
RVN	**6**	
FZI	**4**	

trigrams

Vigenère (Poly-alphabetic Shift) Cipher (1553)

Key: K is a random word of length t.

Encryption Algorithm: Say K= CRYPTO (t=5)

msg	w	h	a	t	a	n	i	c	e	d	a	y	t	o	d	a	y
key	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T
cipher	Z	Z	Z	J	U	C	L	U	D	T	U	N	W	G	C	Q	S

+ mod 26

Exercise:

Think of an attack

Was harder to break. Systematic attack took years to device.

“I got your email. Was it encrypted or is your spelling *that* bad?”