Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

Zhejiang University

3 December 2020

Class 03
More Basic Notions and Some History

Computational Complexity

Cost of performing a computation in instructions, memory locations, gates, dollars, etc. as a function of the size of the input.

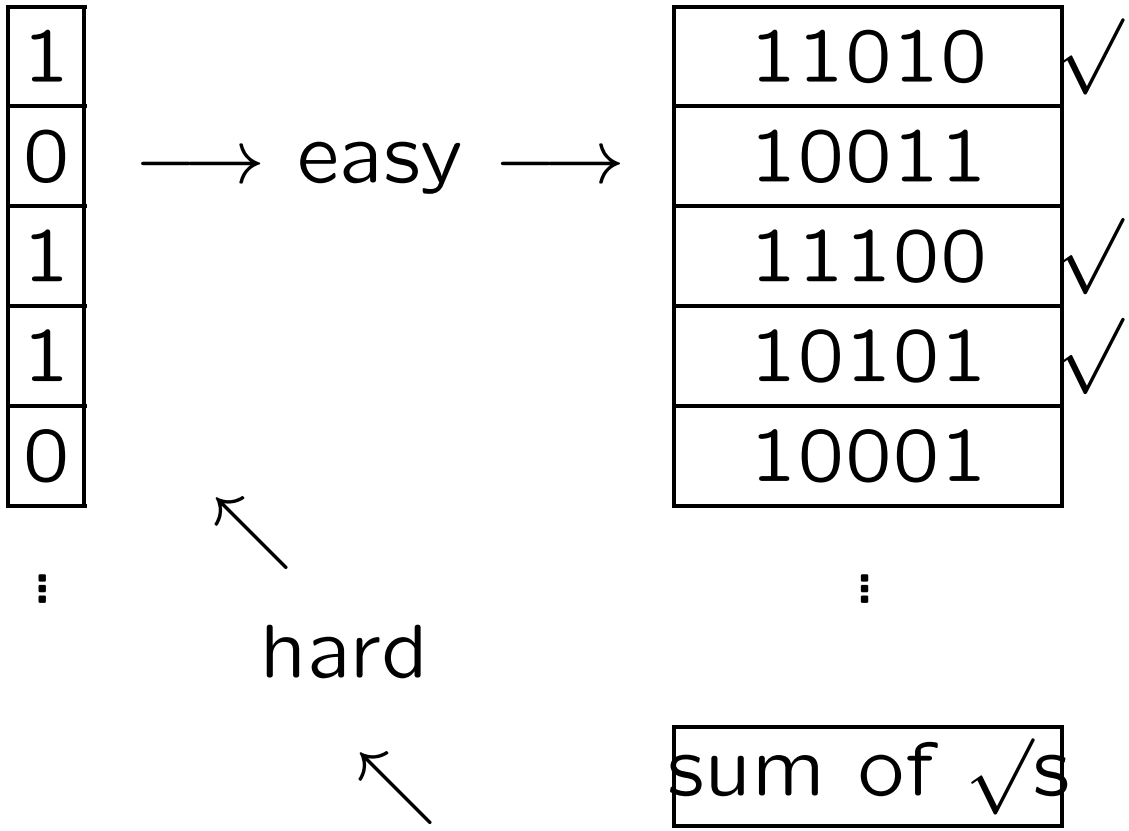
Computational Complexity (Cont'd)

Possible Measures

- Worst Case
- Average Case — Hard to measure

  (What are 'typical' inputs?)
- Easiest Case — Hard to define

Knapsack Problem



Knapsack Problem (Cont'd)

Selecting a subset of the elements of a 'cargo' vector and adding them up is easy.

Given a cargo vector, and a number it is hard to find a subset that add up to that number.

This is an example of a *one-way function, a function that is easy to compute in one direction, but hard to compute in the other.*

Knapsack Problem (Cont'd)

- Worst case is NP-complete.
- Average case is though to be hard but nothing is known for sure.
- Easiest case is trivial: binary decomposition.

Degrees of Difficulty

A problem is considered ‘Easy’ if it can be done in time that is a polynomial function of the length of the input.

Degrees of Difficulty — 2

A problem can be solved in *non-deterministic polynomial time if the answer can be checked in polynomial time. I.e., you could do it in polynomial time if you guessed the answer.*

Degrees of Difficulty — 3

A problem is said to be NP-Complete if any polynomial time technique for solving it could be used to solve all NP-time problems in polynomial time.

Traveling Salesman Problem

The traveling salesman problem:

Find the shortest way of visiting a number of cities, is harder than NP.

Even if you know the answer, you have no easy way of verifying it.

Difficulty of Cryptanalysis

Theorem: The cryptanalytic problem for usable cryptosystems can never be more than NP-hard.

Proof: Encrypt and decrypt in P-time

$\Longrightarrow$ check answer in P-time.

On the other hand, since the knapsack problem is NP-complete, there is an NP-complete cryptanalytic problem.

Criteria of Cryptosystem Performance

- Security
- Cost of Encryption
- Size (Cost) of Key
- Message Expansion
- Error Propagation

The Essence of Security

- Recognition of those you know
- Introduction to those you don't know
- Written Signature
- Private Conversation

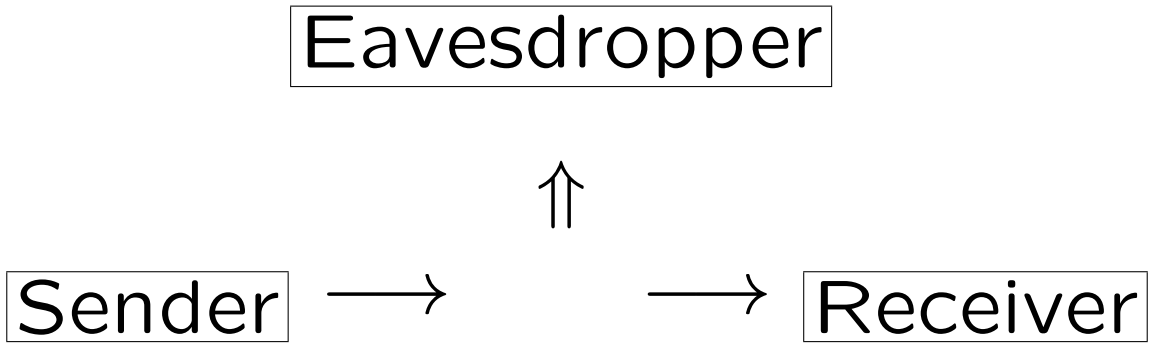
Communication security is the transplantation of these basic social mechanisms to the telecommunications environment.

Privacy or Confidentiality

Guarantee to Sender

Authorized Receivers Only

Channel with Passive Eavesdropper



Other Confidentiality Objectives

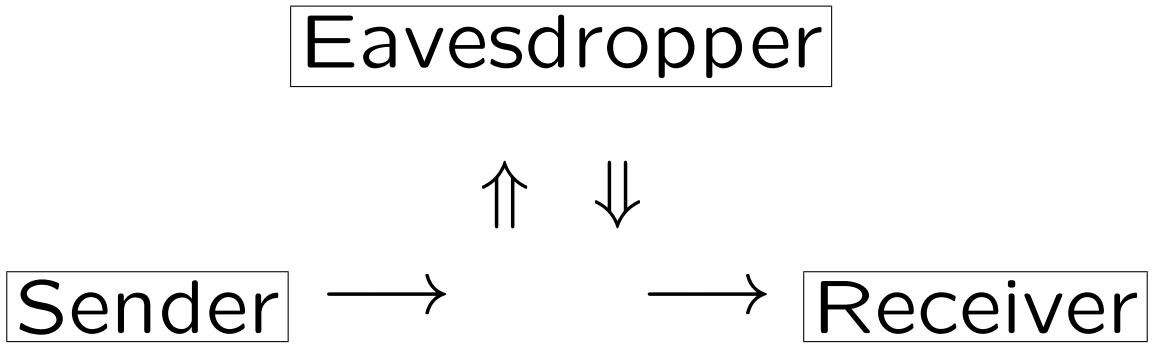
- Transmission Security
- Traffic Confinement

Authenticity and Integrity

Guarantee to Receiver

- Knows Identity of Sender
- Message Not Altered
- Not Unduly Delayed

Channel with Active Eavesdropper



Types of Intrusion

- Message Insertion
- Replay
- Message Deletion
- Denial of Service

Types of Intrusion (cont'd)

- Message Modification
  - With known results
  - With unknown results (e.g., message rearrangement)
- Denial of Service

Confidentiality vs. Authenticity

- EFT — Authenticity
- Satellite Vidoeconference — Confidentiality

Confidentiality and Authenticity Interact

- Phony caller can ask for secret information
- Would be spoofers can read traffic and study network operations.

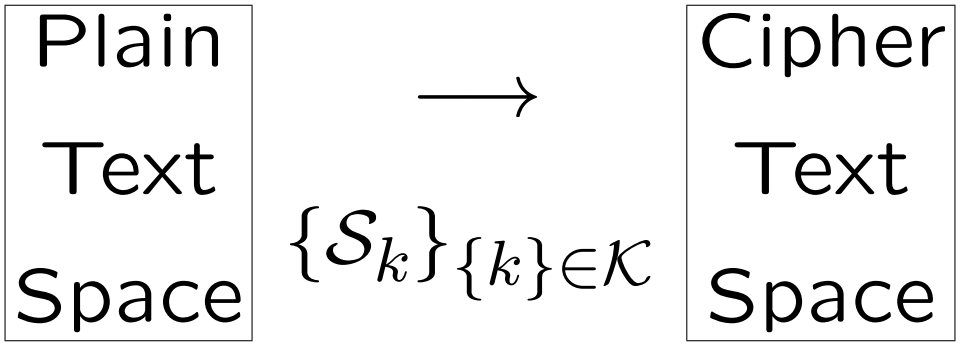
Approaches to Protection

- Pressurized Conduit
- Optical Fiber
- Line of Sight Laser
- Damped frequencies
- Spread Spectrum
- Cryptography

Cryptography

Protection of data by transformations that turn useful and comprehensible plaintext into scrambled and meaningless ciphertext under control of secret keys.

Cryptographic System



Cryptography Guarantees Confidentiality

- Only authorized receivers who know secret keys can decrypt
- Eavesdropper may intercept message, but cannot understand it.

Cryptography Guarantees Authenticity

- Message sent by Intruder will decrypt to nonsense.
- Intruder may inject messages, but cannot 'get them accepted.'

Origins of Cryptography

- The basic ideas are not new.
- 200AH — Al Kindi in Baghdad
- 1500AD — Alberti et al. in Italy

Polyalphabetic Ciphers

- Substitution must change from character to character

Homophonic Substitution

The ciphertext is not uniquely determined by the plaintext. P goes to:

- C_{11} or C_{12} or $C_{13}\ldots$ under K_1
- C_{21} or C_{22} or $C_{23}\ldots$ under K_2
- C_{31} or C_{32} or $C_{33}\ldots$ under K_3
- etc.

(This is not a mapping)

Basics of Symmetric Cryptography

- Two ideas: arithmetic and table lookup
- Q: Why so slow to develop?
- A: You couldn't really do them without machine computing.

Pre-machine Ciphers

- Codes dominate
- Vigenère and multiple Vigenère
- Playfair — 19th Century
- ADFGVX — WWI

Addition Modulo n

Two numbers are added modulo n by adding them as integers and subtracting n if the result is larger than n. For example $19 + 7 = 2 \pmod{12}$.

Addition Modulo n (Cont'd)

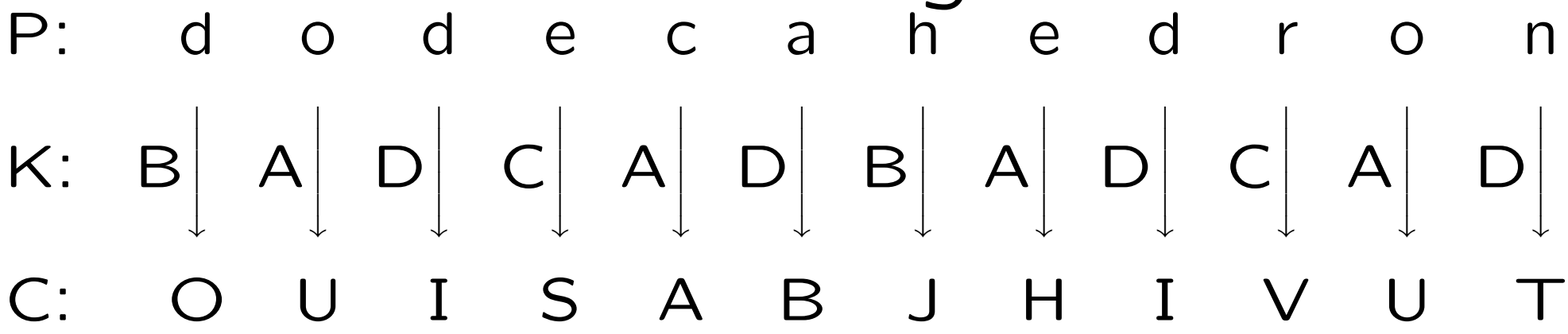
Addition modulo 26 can be used to combine letters of the alphabet in a manner equivalent to the substitution alphabets above by setting $A = 0$, $B = 1$, $C = 2$, ..., $z = 25$.

Vigenère System with Full Substitution

The primary key is a list of *cipher alphabets that will be applied sequentially to the plaintext, starting over again when the list is exhausted.*

The secondary key is the set of cipher alphabets from which this list is drawn.

Effect of Vigenère



'd' is carried to 'O' under the 'B' alphabet; 'o' is carried to 'U' under the 'A' alphabet; 'd' is carried to 'I' under the 'D' alphabet; etc.

Vigenère Table (Secondary Key)

	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
A	Q	F	A	L	H	I	M	Z	E	T	Y	N	B	O	U	D	X	P	C	S	K	G	R	J	V	W
B	Y	L	K	O	R	U	C	J	X	P	A	S	V	H	B	D	Q	G	M	I	T	E	Z	J	W	N
C	J	O	A	M	S	I	T	Y	R	D	N	H	X	E	W	P	F	V	Z	B	L	G	K	Q	U	C
D	B	H	X	I	E	W	L	P	C	R	V	A	F	T	S	M	U	N	Q	K	Z	D	G	O	Y	J
E	O	E	N	F	G	D	H	Z	J	B	R	I	S	Y	V	W	T	X	U	L	P	K	Q	A	C	M
⋮										.		.		.												

Vigenère Table with Cyclic Alphabets

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
⋮										.			.				.									

Vigenère with Cyclic Substitution

Plain:	`HENRY IS HUNGRY ...`
Key:	`PAPAD UM PAPADU ...`
Cipher:	`WECRB CE WUCGUS ...`

Double Vigenère System

Plain:	`HENRY IS HUNGRY ...`
Key-1:	`PAPAD UM PAPADU ...`
Cipher-1:	`WECRB CE WUCGUS ...`
Key-2:	`HIPSH IP SHIPSH ...`
Cipher-2:	`DMRJI KT OBKVMZ ...`

This brings us to the eve of World War I. Next time we will begin looking at 20th Century cryptography.