CS201 DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. QI WANG

Department of Computer Science and Engineering
Office: Room413, CoE South Tower
Email: wangqi@sustech.edu.cn

Applications of Number Theory in Cryptography

- Introduction
- Symmetric cryptography
- Asymmetric cryptography
- RSA Cryptosystem
- DLP and El Gamal cryptography
- Diffie-Hellman key exchange protocol
- Crytocurrency, e.g., bitcoin

Cryptography

- History of almost 4000 years (from 1900 B.C.)

$$\text{Cryptography} = \text{kryptos} + \text{graphos}$$

Cryptography

- History of almost 4000 years (from 1900 B.C.)

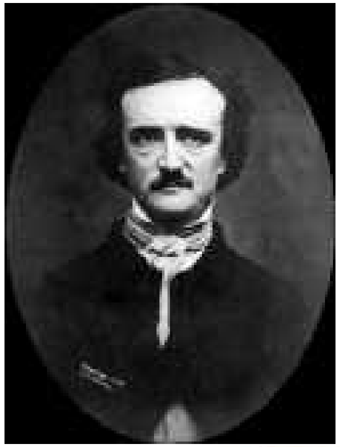
$$\text{Cryptography} = \underset{(\text{secret})}{\text{kryptos}} + \underset{(\text{writing})}{\text{graphos}}$$

Cryptography

- History of almost 4000 years (from 1900 B.C.)

Cryptography = kryptos + graphos
(secret) (writing)

The term was first used in *The Gold-Bug*, by Edgar Allan Poe (1809 - 1849).

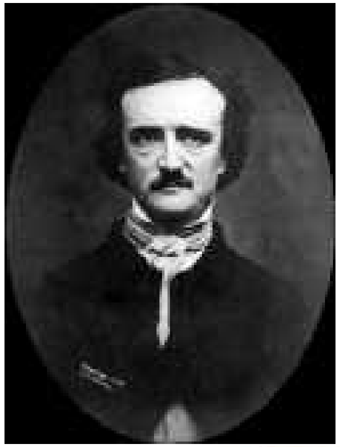


Cryptography

- History of almost 4000 years (from 1900 B.C.)

Cryptography = kryptos + graphos
(secret) (writing)

The term was first used in *The Gold-Bug*, by Edgar Allan Poe (1809 - 1849).



"Human ingenuity cannot concoct a cipher which human ingenuity cannot resolve." – 1841

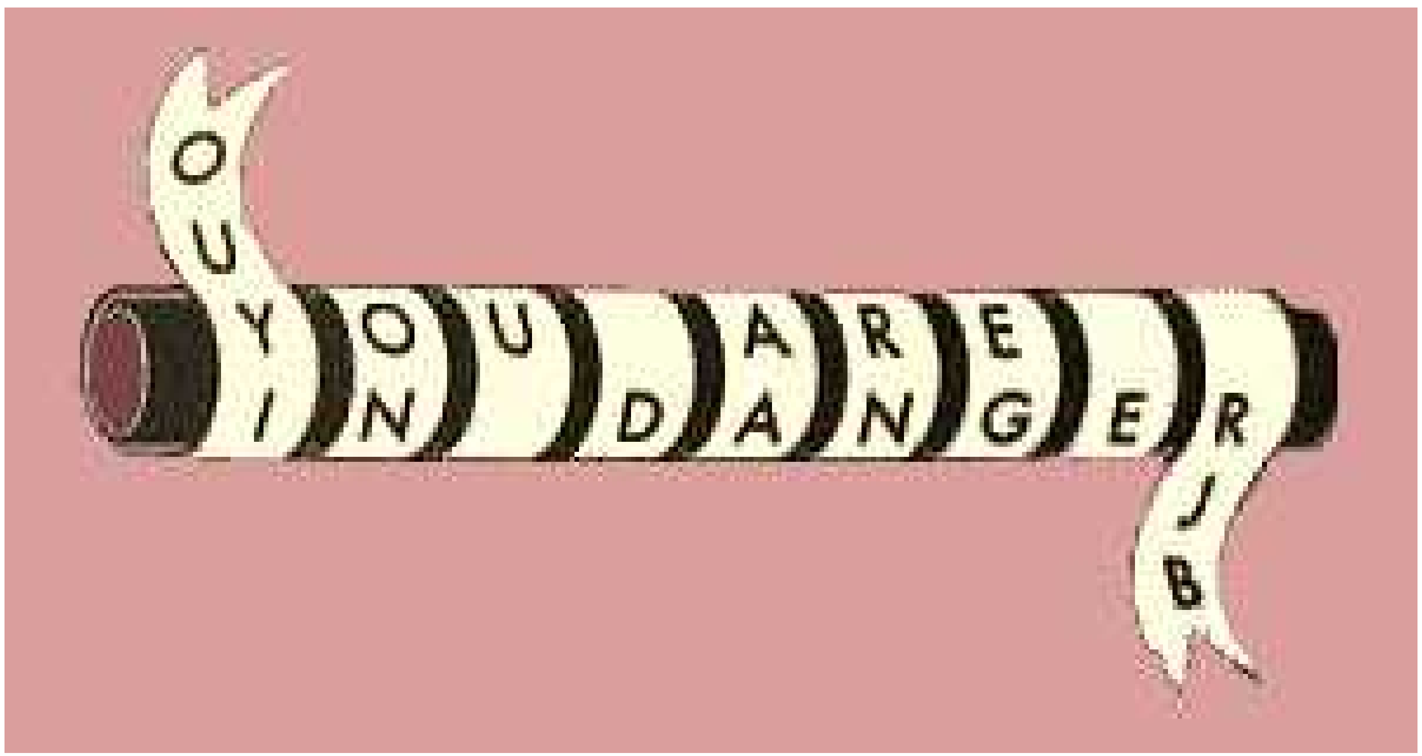
Cryptography

- One-sentence definition:

  "Cryptography is the practice and study of techniques for secure communication in the presence of third parties called *adversaries*." – Ronald L. Rivest

Some Examples

- In 405 BC, the Greek general LYSANDER OF SPARTA was sent a coded message written on the inside of a servant's belt.



Some Examples

- The Greeks also invented a cipher which changed letters to numbers. A form of this code was still being used during *World War I*.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Some Examples

- Caesar Cipher (after the name of JULIUS CAESAR)

VENI, VIDI, VICI

YHQL YLGL YLFL

Some Examples

- Morse Code: created by Samuel Morse in 1838

Morse Alphabet

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

Full stop (.) • — • — • —
Break signal or fresh line — • • • —
Apostrophe (') • — — — — •
Hyphen (-) — • • • • —
Exclamation (!) — — • • — —
Interrogation (?) • • — — • •
Underline (———) • • — — • —
Parenthesis ( ) — • — — • —
Inverted commas (“ ”) • — • • — •

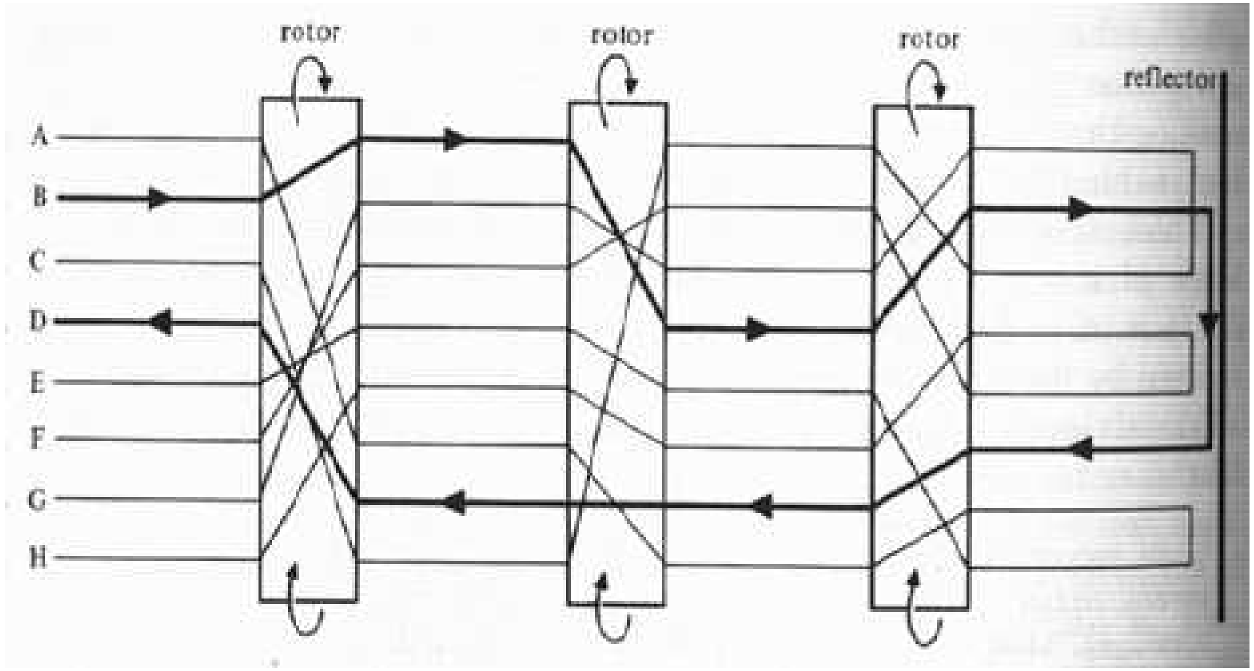
Some Examples

- Crytograms from the Chinese gold bars

http://www.iacr.org/misc/china/china.html

Some Examples

- Enigma, Germany coding machine in *World War II.*



Some Examples

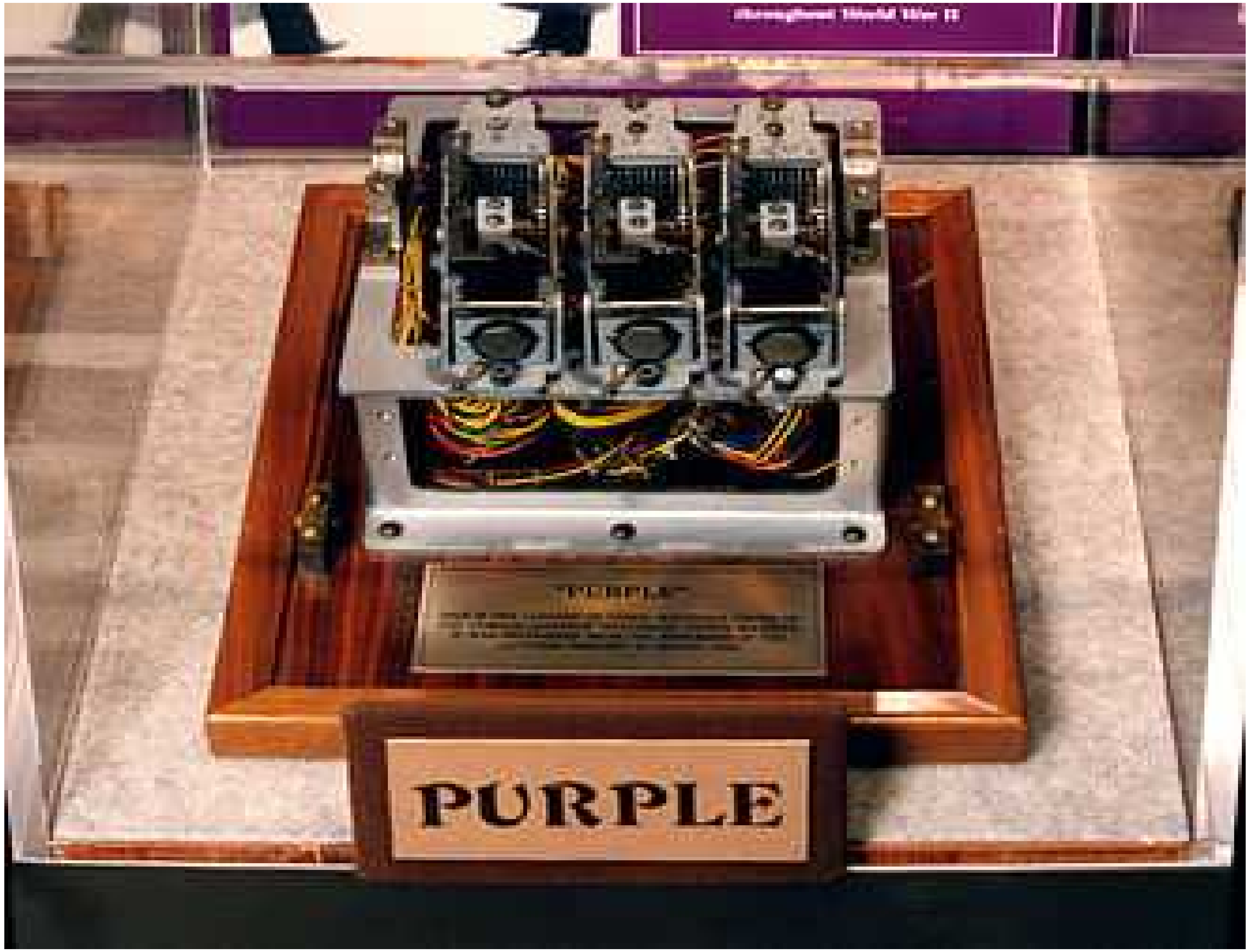
- Sigaba, used by U.S. during *World War II.*

Some Examples

- Japanese "Enigma" Rotor Cipher Machine

Some Examples

- Japanese Purple Machine (97-shiki obun inji-ki)



People Working in Breaking Codes

Alan Turing
(1912-1954)

Claude E. Shannon
(1916-2001)

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

They need agree in advance on the secret key k.

Cryptography History

- History (until 1970's)

"*Symmetric*" cryptography

They need agree in advance on the secret key k.

$\mathcal{Q}$: How can they do this?

Cryptography History

- History (until 1970's)

  "*Symmetric*" cryptography

They need agree in advance on the secret key k.

$\mathcal{Q}$: How can they do this?

$\mathcal{Q}$: What if Bob could send Alice a "special key" useful only for encryption but no help for decryption?

Caesar Cipher

- Key: $k = 0, 1, \ldots, 25$

  Encryption: encode i as $(i + k) \bmod 26$

  Decryption: decode j as $(j - k) \bmod 26$

Caesar Cipher

- Key: $k = 0, 1, \ldots, 25$

  Encryption: encode i as $(i + k) \bmod 26$

  Decryption: decode j as $(j - k) \bmod 26$

  plaintext: SEND REINFORCEMENT
  Key: 2
  ciphertext: UGPF TGKPHQTEGOGPV

Caesar Cipher

- Key: $k = 0, 1, \ldots, 25$

  Encryption: encode i as $(i + k) \bmod 26$

  Decryption: decode j as $(j - k) \bmod 26$

  plaintext: SEND REINFORCEMENT
  Key: 2
  ciphertext: UGPF TGKPHQTEGOGPV

  Problem: only 26 possibilities for keys!

Caesar Cipher

- Key: $k = 0, 1, \ldots, 25$

  Encryption: encode i as $(i + k) \bmod 26$

  Decryption: decode j as $(j - k) \bmod 26$

  plaintext: SEND REINFORCEMENT
  Key: 2
  ciphertext: UGPF TGKPHQTEGOGPV

  Problem: only 26 possibilities for keys!

  Kerchoff's Principle (1883): System should be secure even if algorithms are known, as long as key is secret.

Substitution Cipher

- Key: table mapping each letter to another letter

A	B	C		Z
V	R	E		D

Substitution Cipher

- Key: table mapping each letter to another letter

A	B	C		Z
V	R	E		D

Encryption & Decryption: letter by letter according to table

Substitution Cipher

- Key: table mapping each letter to another letter

A	B	C		Z
V	R	E		D

Encryption & Decryption: letter by letter according to table

# of possible keys: $26! \approx 4 \times 10^{26}$

Substitution Cipher

- Key: table mapping each letter to another letter

A	B	C		Z
V	R	E		D

Encryption & Decryption: letter by letter according to table

# of possible keys: $26! \approx 4 \times 10^{26}$

However, substitution cipher is still insecure!

Substitution Cipher

- Key: table mapping each letter to another letter

A	B	C		Z
V	R	E		D

Encryption & Decryption: letter by letter according to table

\# of possible keys: $26! \approx 4 \times 10^{26}$

However, substitution cipher is still insecure!

Key observation: can recover plaintext using *statistics* on *letter frequencies.*

Substitution Cipher

Table 1: Relative frequencies of the letters of the English language

Letter	Relative Frequency (%)	Letter	Relative Frequency (%)
a	8.167	n	6.749
b	1.492	o	7.507
c	2.782	p	1.929
d	4.253	q	0.095
e	12.702	r	5.987
f	2.228	s	6.327
g	2.015	t	9.056
h	6.094	u	2.758
i	6.966	v	0.978
j	0.153	w	2.360
k	0.772	x	0.150
l	4.025	y	1.974
m	2.406	z	0.074

Substitution Cipher

Table 2: Number of Diagraphs Expected in 2,000 Letters of English Text

th	-	50	at	-	25	st	-	20
er	-	40	en	-	25	io	-	18
on	-	39	es	-	25	le	-	18
an	-	38	of	-	25	is	-	17
re	-	36	or	-	25	ou	-	17
he	-	33	nt	-	24	ar	-	16
in	-	31	ea	-	22	as	-	16
ed	-	30	ti	-	22	de	-	16
ne	-	30	to	-	22	rt	-	16
ha	-	26	it	-	20	ve	-	16

Table 3: The 15 Most Common Trigraphs in the English Language

1	-	the	6	-	tio	11	-	edt
2	-	and	7	-	for	12	-	tis
3	-	tha	8	-	nde	13	-	oft
4	-	ent	9	-	has	14	-	sth
5	-	ion	10	-	nce	15	-	men

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL MGLMXQERIWGPSRIHMXQEREKI

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL MGLMXQERIWGPSRIHMXQEREKI

  I – *most common letter*
  LI – *most common pair*
  XLI – *most common triple*

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL MGLMXQERIWGPSRIHMXQEREKI

I – *most common letter* $\quad$ I $=$ e

LI – *most common pair* $\quad$ L $=$ h

XLI – *most common triple* $\quad$ X $=$ t

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL MGLMXQERIWGPSRIHMXQEREKI

I – *most common letter*
LI – *most common pair*
XLI – *most common triple*

I = e
L = h
X = t

LIVI = he?e

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKI

I – *most common letter* I = e
LI – *most common pair* L = h
XLI – *most common triple* X = t

LIVI = he?e V = r

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL MGLMXQERIWGPSRIHMXQEREKI

I – *most common letter*
LI – *most common pair*
XLI – *most common triple*

LIVI = he?e

I = e
L = h
X = t

V = r
E = a
Y = g

Substitution Cipher

- LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFE MVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQL MGLMXQERIWGPSRIHMXQEREKI

I – *most common letter*
LI – *most common pair*
XLI – *most common triple*

LIVI = he?e

I = e
L = h
X = t

V = r
E = a
Y = g

HereUpOnLeGrandAroseWithAGraveAndStatelyAirAndBroug MeTheBeetleFromAGlassCaseInWhichItWasEnclosedIt-WasABe

- History (from 1976)
  - ◇ W. Diffie, M. Hellman, "New direction in cryptography", *IEEE Transactions on Information Theory, vol. 22, pp. 644-654, 1976.*

"We stand today on the brink of a revolution in cryptography."

Bailey W. Diffie

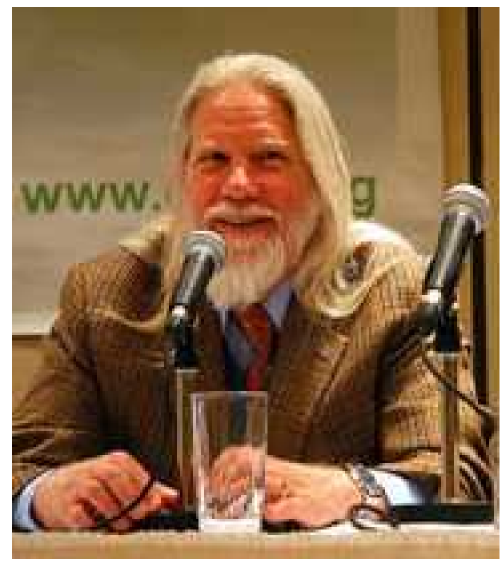
Martin E. Hellman

Cryptography History

- History (from 1976)
  - ◇ W. Diffie, M. Hellman, “New direction in cryptography”, *IEEE Transactions on Information Theory, vol. 22, pp. 644-654, 1976.*

“We stand today on the brink of a revolution in cryptography.”

2015 **Turing Award**



Bailey W. Diffie

Martin E. Hellman

2015	Martin E. Hellman Whitfield Diffie	For fundamental contributions to **modern cryptography**. Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography,"[39] introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the internet today.[40]

Public Key Cryptography

- Alice wants to send a message to Bob

Public Key Cryptography

- Alice wants to send a message to Bob

Public Key Cryptography

- Alice wants to send a message to Bob

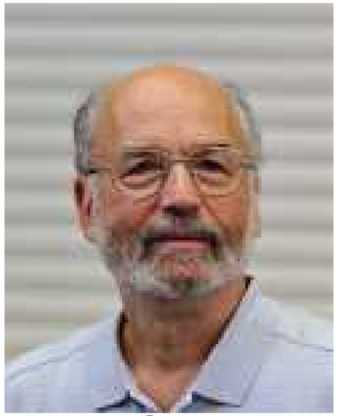
Public Key Cryptography

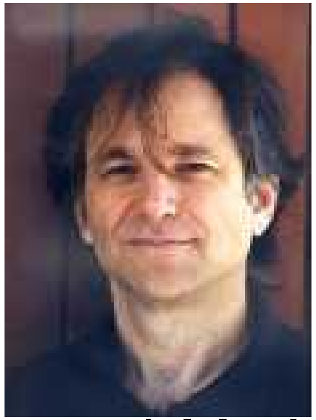
- Alice wants to send a message to Bob

Public Key Cryptography

- Alice wants to send a message to Bob


Ronald L. Rivest


Adi Shamir


Leonard M. Adleman

R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21-2, pages 120-126, 1978.

RSA Public Key Cryptosystem

- **R**ivest-**S**hamir-**A**dleman 2002 **Turing Award**

2002	Ronald L. Rivest, Adi Shamir and Leonard M. Adleman	For their ingenious contribution for making **public-key cryptography** useful in practice.

RSA Public Key Cryptosystem

- **R**ivest-**S**hamir-**A**dleman 2002 **Turing Award**

2002	Ronald L. Rivest, Adi Shamir and Leonard M. Adleman	For their ingenious contribution for making **public-key cryptography** useful in practice.

Pick two large primes, p and q. Let $n = pq$, then $\phi(n) = (p-1)(q-1)$. Encryption and decryption keys e and d are selected such that

- $\gcd(e, \phi(n)) = 1$
- $ed \equiv 1 \pmod{\phi(n)}$

RSA Public Key Cryptosystem

- **R**ivest-**S**hamir-**A**dleman 2002 **Turing Award**

2002	Ronald L. Rivest, Adi Shamir and Leonard M. Adleman	For their ingenious contribution for making public-key cryptography useful in practice.

Pick two large primes, p and q. Let $n = pq$, then $\phi(n) = (p-1)(q-1)$. Encryption and decryption keys e and d are selected such that

- $\gcd(e, \phi(n)) = 1$
- $ed \equiv 1 \pmod{\phi(n)}$

$C = M^e \bmod n$ (RSA **encryption)**

$M = C^d \bmod n$ (RSA **decryption)**

RSA Public Key Cryptosystem

- $C = M^e \bmod n$ (RSA **encryption)**

  $M = C^d \bmod n$ (RSA **decryption)**

Theorem (*Correctness*) : Let p and q be two odd primes, and define $n = pq$. Let e be relatively prime to $\phi(n)$ and let d be the multiplicative inverse of e modulo $\phi(n)$. For each integer x such that $0 \le x < n$,

$$x^{ed} \equiv x \pmod{n}.$$

RSA Public Key Cryptosystem

- $C = M^e \bmod n$ (RSA **encryption)**

  $M = C^d \bmod n$ (RSA **decryption)**

Theorem (*Correctness*) : Let p and q be two odd primes, and define $n = pq$. Let e be relatively prime to $\phi(n)$ and let d be the multiplicative inverse of e modulo $\phi(n)$. For each integer x such that $0 \leq x < n$,

$$x^{ed} \equiv x \pmod{n}.$$

$\mathcal{Q}$: How to prove this?

RSA Public Key Cryptosystem: Example

Parameters:	p	q	n	$\phi(n)$	e	d
	5	11	55	40	7	23

RSA Public Key Cryptosystem: Example

Parameters:	p	q	n	$\phi(n)$	e	d
	5	11	55	40	7	23

Public key: $(7, 55)$

Private key: 23

RSA Public Key Cryptosystem: Example

Parameters:	p	q	n	$\phi(n)$	e	d
	5	11	55	40	7	23

Public key: $(7, 55)$

Private key: 23

Encryption: $M = 28, C = M^7 \bmod 55 = 52$

Decryption: $M = C^{23} \bmod 55 = 28$

RSA Public Key Cryptosystem: Parameters

Parameters: p q n $\phi(n)$ e d

Public key: (e, n)

Private key: d

p, q, $\phi(n)$ must be kept secret!

RSA Public Key Cryptosystem: Parameters

Parameters: p q n $\phi(n)$ e d

Public key: (e, n)

Private key: d

p, q, $\phi(n)$ must be kept secret!

$\mathcal{Q}$: Why?

RSA Public Key Cryptosystem: Parameters

Parameters: $p \quad q \quad n \quad \phi(n) \quad e \quad d$

Public key: (e, n)

Private key: d

p, q, $\phi(n)$ must be kept secret!

$\mathcal{Q}$: Why?

Comment: It is believed that determining $\phi(n)$ is equivalent to factoring n. Meanwhile, determining d given e and n, appears to be at least as time-consuming as the integer factoring problem.

Parameters: $p \quad q \quad n \quad \phi(n) \quad e \quad d$

Public key: (e, n)

Private key: d

p, q, $\phi(n)$ must be kept secret!

$\mathcal{Q}$: Why?

Comment: It is believed that determining $\phi(n)$ is equivalent to factoring n. Meanwhile, determining d given e and n, appears to be at least as time-consuming as the integer factoring problem.

The Security of the RSA

In practice, RSA keys are typically 1024 to 2048 bits long.

The Security of the RSA

In practice, RSA keys are typically 1024 to 2048 bits long.

Remark: There are some suggestions for choosing p and q.

A. Salomaa, *Public-Key Cryptography*, 2nd Edition, Springer, 1996, pp. 134-136.

The Security of the RSA

In practice, RSA keys are typically 1024 to 2048 bits long.

Remark: There are some suggestions for choosing p and q.

A. Salomaa, *Public-Key Cryptography*, 2nd Edition, Springer, 1996, pp. 134-136.

$\mathcal{Q}$: Consider the RSA system, where $n = pq$ is the modulus. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work?

Applications of RSA

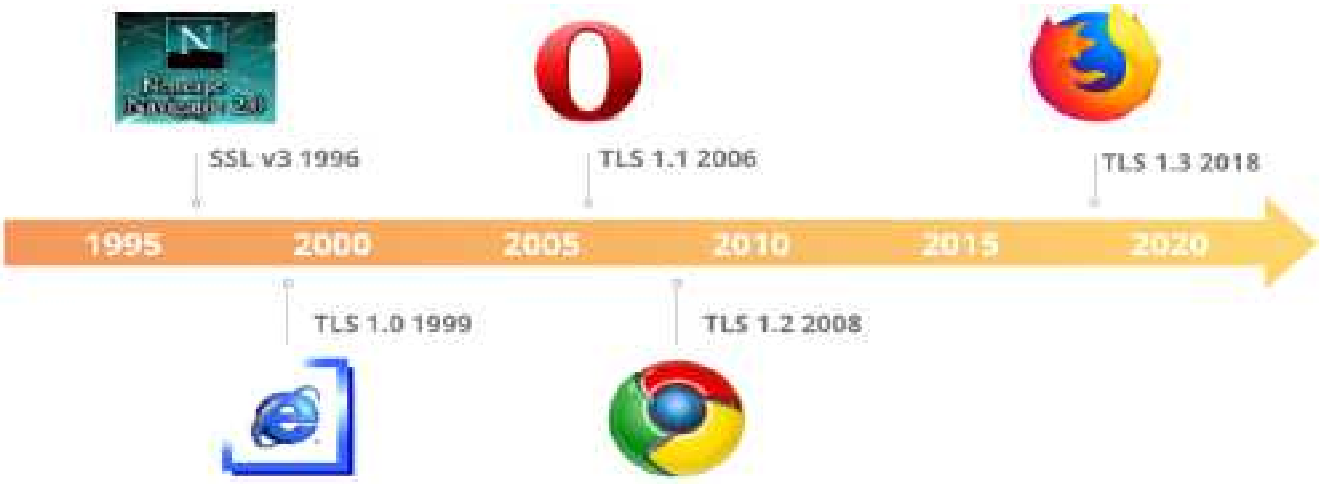
- SSL/TLS protocol

Applications of RSA

- SSL/TLS protocol

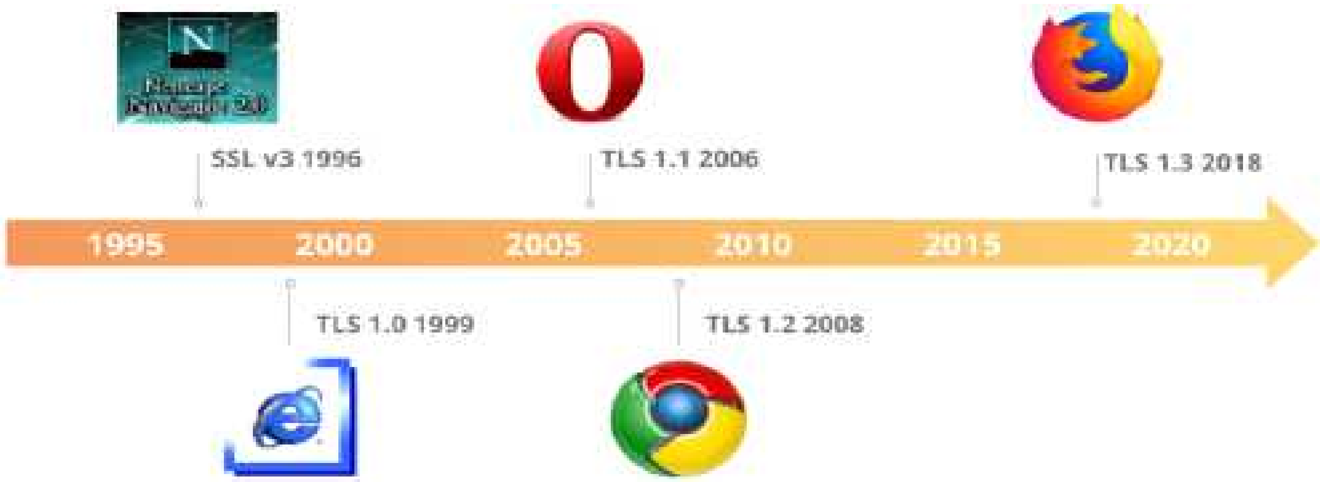
Applications of RSA

- SSL/TLS protocol



Applications of RSA

- SSL/TLS protocol

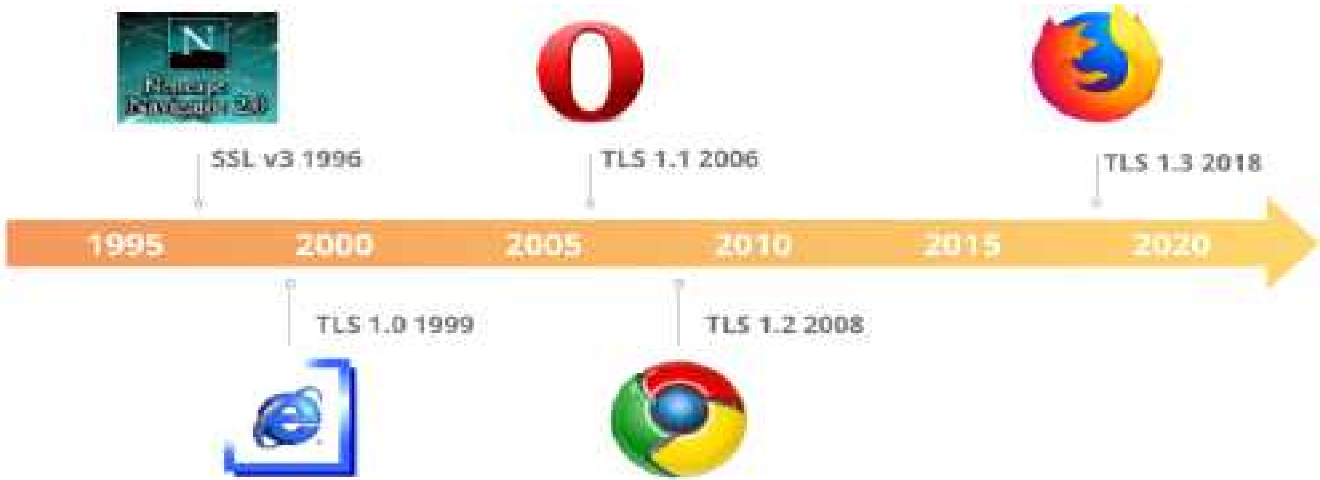


Key exchange/agreement and authentication

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes

Applications of RSA

- SSL/TLS protocol

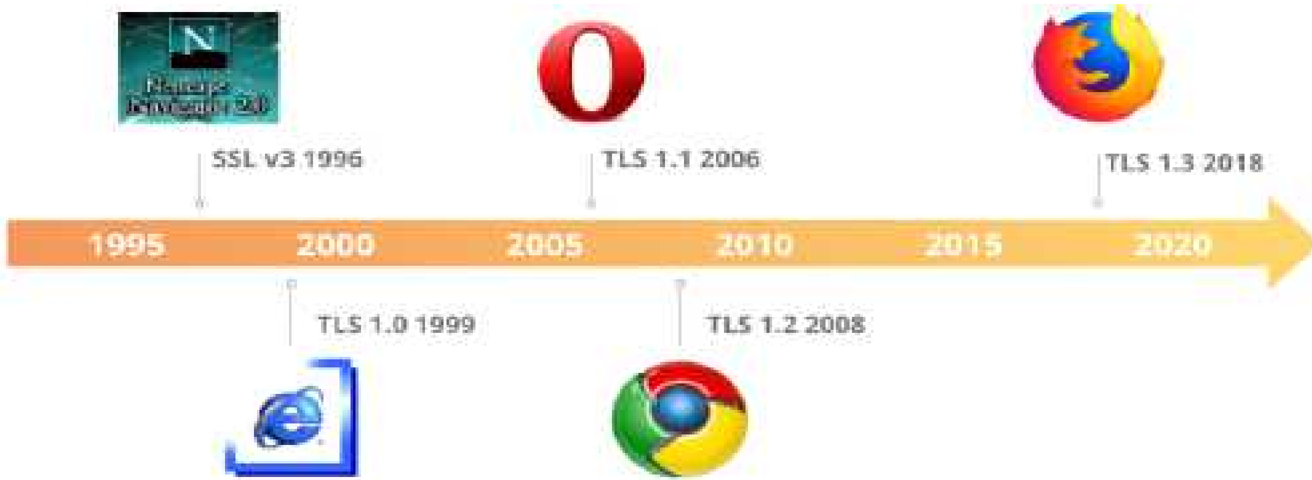


Key exchange/agreement and authentication

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes

Applications of RSA

- SSL/TLS protocol



Key exchange/agreement and authentication

Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
RSA	Yes	Yes	Yes	Yes	Yes	No
DH-RSA	No	Yes	Yes	Yes	Yes	No
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes
ECDH-RSA	No	No	Yes	Yes	Yes	No
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes

Using RSA for Digital Signature

$S = M^d \bmod n$ (RSA **signature)**

$M = S^e \bmod n$ (RSA **verification)**

Why?

The Discrete Logrithm

- **The discrete logarithm** of an integer y to the base b is an integer x, such that

$$b^x \equiv y \bmod n.$$

- **The discrete logarithm** of an integer y to the base b is an integer x, such that

$$b^x \equiv y \bmod n.$$

Discrete Logarithm Problem:

Given n, b and y, find x.

- **The discrete logarithm** of an integer y to the base b is an integer x, such that

$$b^x \equiv y \bmod n.$$

Discrete Logarithm Problem:

Given n, b and y, find x.

This is very hard!

El Gamal Encryption

- **Setup** Let p be a prime, and g be a generator of $\mathbb{Z}_p$. The private key x is an integer with $1 < x < p - 2$. Let $y = g^x \bmod p$. The public key for *El Gamal encryption* is (p, g, y).

- **Setup** Let p be a prime, and g be a generator of $\mathbb{Z}_p$. The private key x is an integer with $1 < x < p - 2$. Let $y = g^x \bmod p$. The public key for *El Gamal encryption* is (p, g, y).

  El Gamal Encryption: Pick a random integer k from $\mathbb{Z}_{p-1}$,

  $$a = g^k \bmod p$$
  $$b = My^k \bmod p$$

  The ciphertext C consists of the pair (a, b).

  El Gamal Decryption:

  $$M = b(a^x)^{-1} \bmod p$$

Using El Gamal for Digital Signature

$$a = g^k \bmod p$$
$$b = k^{-1}(M - xa) \bmod (p-1)$$

(El Gamal **signature**)

$$y^a a^b \equiv g^M \pmod{p}$$

(El Gamal **verification**)

Using El Gamal for Digital Signature

$$a = g^k \bmod p$$
$$b = k^{-1}(M - xa) \bmod (p-1)$$

(El Gamal **signature**)

$$y^a a^b \equiv g^M \pmod{p}$$

(El Gamal **verification**)

$\mathcal{Q}$: How to verify it?

An Example

Choose $p = 2579$, $g = 2$, and $x = 765$. Hence $y = 2^{765} \bmod 2579 = 949$.

An Example

Choose $p = 2579$, $g = 2$, and $x = 765$. Hence $y = 2^{765} \bmod 2579 = 949$.

- **(Public key)** $k_e = (p, g, y) = (2579, 2, 949)$
- **(Private key)** $k_d = x = 765$

An Example

Choose $p = 2579$, $g = 2$, and $x = 765$. Hence $y = 2^{765} \bmod 2579 = 949$.

- **(Public key)** $k_e = (p, g, y) = (2579, 2, 949)$
- **(Private key)** $k_d = x = 765$

Encryption: Let $M = 1299$ and choose a random $k = 853$,

$$\begin{aligned}(a, b) &= (g^k \bmod p, My^k \bmod p)\\ &= (2^{853} \bmod 2579, 1299 \cdot 949^{853} \bmod 2579)\\ &= (435, 2396).\end{aligned}$$

Decryption:

$$M = b(a^x)^{-1} \bmod p = 2396 \times (435^{765})^{-1} \bmod 2579 = 1299.$$

Question 1: Is it feasible to derive x from (p, g, y)?

Question 1: Is it feasible to derive x from (p, g, y)?

It is equivalent to solving the DLP. It is believed that there is NO polynomial-time algorithm. p should be large enough, typically 160 bits.

Question 1: Is it feasible to derive x from (p, g, y)?

It is equivalent to solving the DLP. It is believed that there is NO polynomial-time algorithm. p should be large enough, typically 160 bits.

Question 2: Given a ciphertext (a, b), is it feasible to derive the plaintext M?

Security of the El Gamal Cryptosystem

Question 1: Is it feasible to derive x from (p, g, y)?

It is equivalent to solving the DLP. It is believed that there is NO polynomial-time algorithm. p should be large enough, typically 160 bits.

Question 2: Given a ciphertext (a, b), is it feasible to derive the plaintext M?

Attack 1: Use $M = by^{-k}$. However, k is randomly picked.

Attack 2: Use $M = b(a^x)^{-1} \bmod p$, but x is secret.

Diffie-Hellman Key Exchange Protocol

User A		User B
Generate random $X_A < p$ calculate $Y_A = \alpha^{X_A} \bmod p$ Calculate $k = (Y_B)^{X_A} \bmod p$	$\xrightarrow{Y_A}$ $\xleftarrow[Y_B]{}$	Generate random $X_B < p$ Calculate $Y_B = \alpha^{X_B} \bmod p$ Calculate $k = (Y_A)^{X_B} \bmod p$

Cryptography Wonders

- *Digital Signatures*. Electronically sign documents

  Zero-knowledge Proofs. Alice proves to Bob that she earns $< \$50k$ without Bob learning her income.

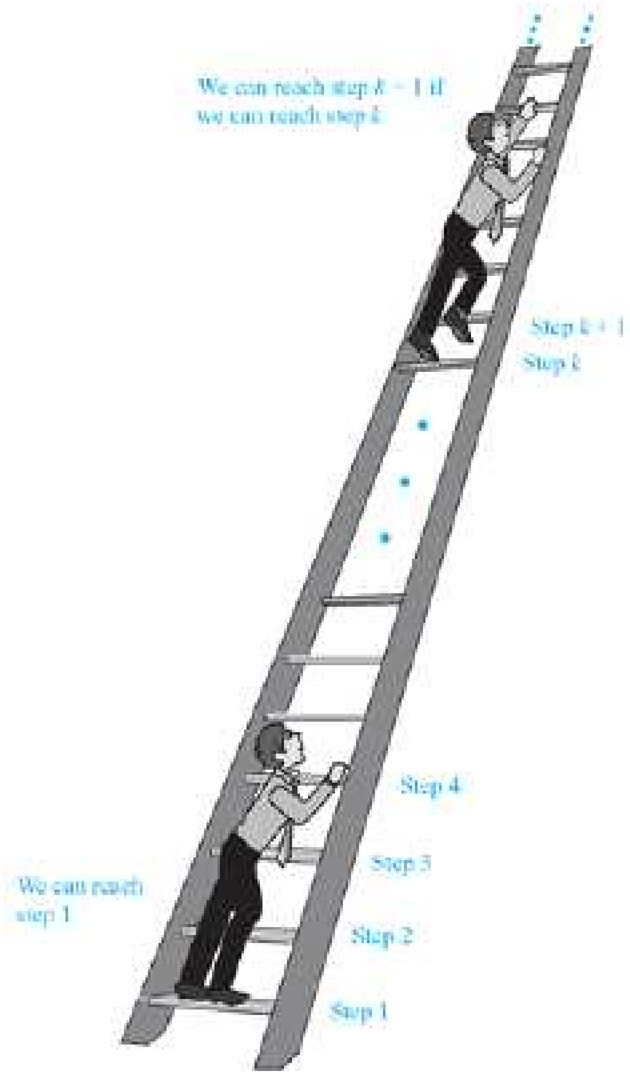
  Privacy-perserving data mining. Bob holds DB. Alice gets answer to one query, without Bob knowing what she asked.

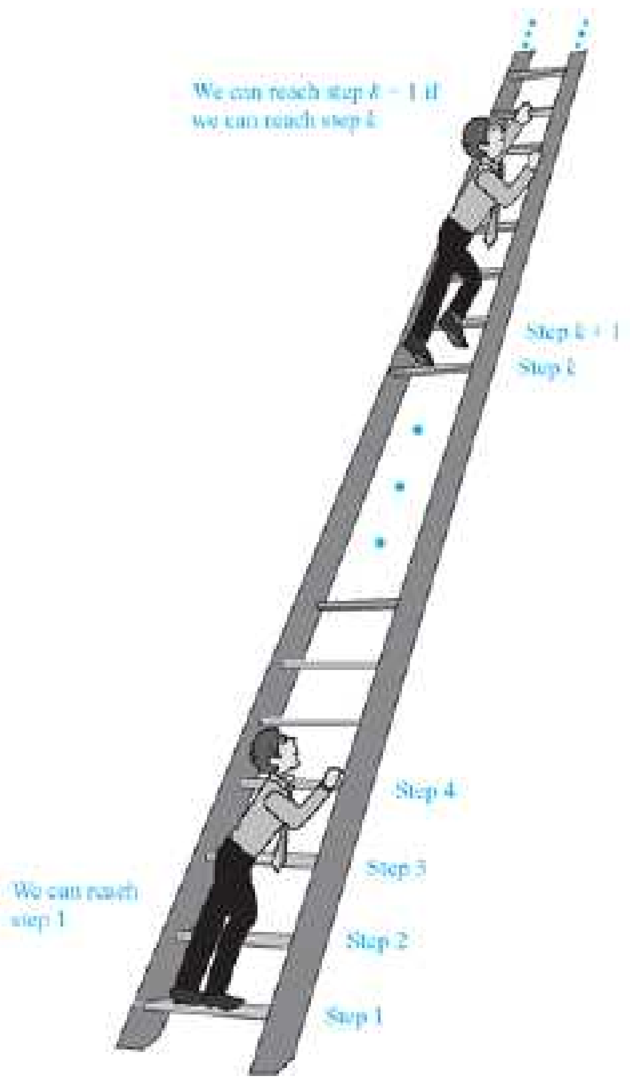
  Playing poker over the net. Alice, Bob, Carol and David can play Poker over the net without trusting each other or any central server. (*E-Voting*)

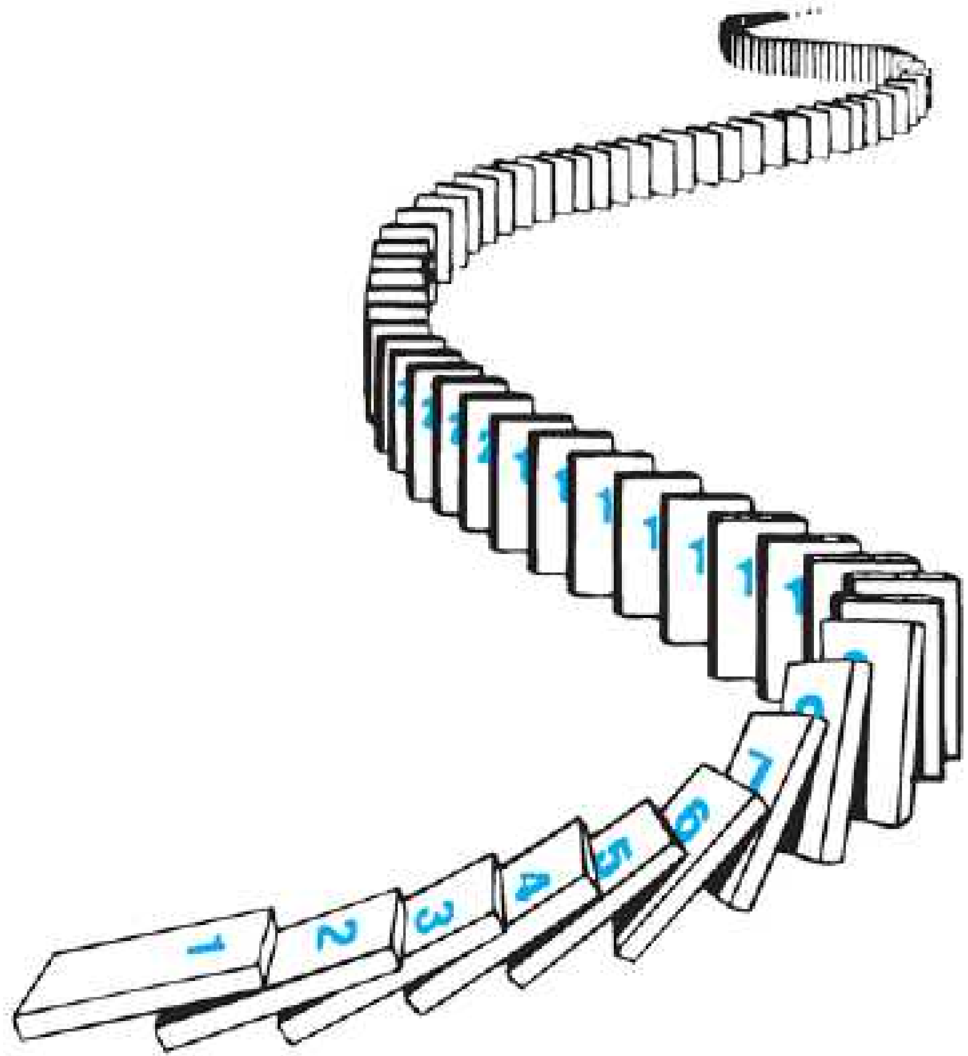
  Electronic Auctions. Can run auctions s.t. no one (even not seller) learns anything other than winning party and bid.

  Fully Homomorphic Encryption. Encrypt $E(m)$ in a way that allows to compute $E(f(m))$.

Mathematical Induction




We can reach step k + 1 if
we can reach step k
Step k + 1
Step k
Step 4
Step 3
We can reach
step 1
Step 2
Step 1



Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

- This leads us to transform the *indirect proof* of proof by counterexample to *direct proof*. This direct proof technique will be **induction**.

Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

- This leads us to transform the *indirect proof* of proof by counterexample to *direct proof*. This direct proof technique will be **induction**.

- We conclude by distinguishing between the *weak principle* of mathematical induction and the *strong principle* of mathematical induction.

Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

- This leads us to transform the *indirect proof* of proof by counterexample to *direct proof*. This direct proof technique will be **induction**.

- We conclude by distinguishing between the *weak principle* of mathematical induction and the *strong principle* of mathematical induction.

  The *strong principle* can actually be derived from the *weak principle*.

Proof by Smallest Counterexample

- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

Proof by Smallest Counterexample

- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

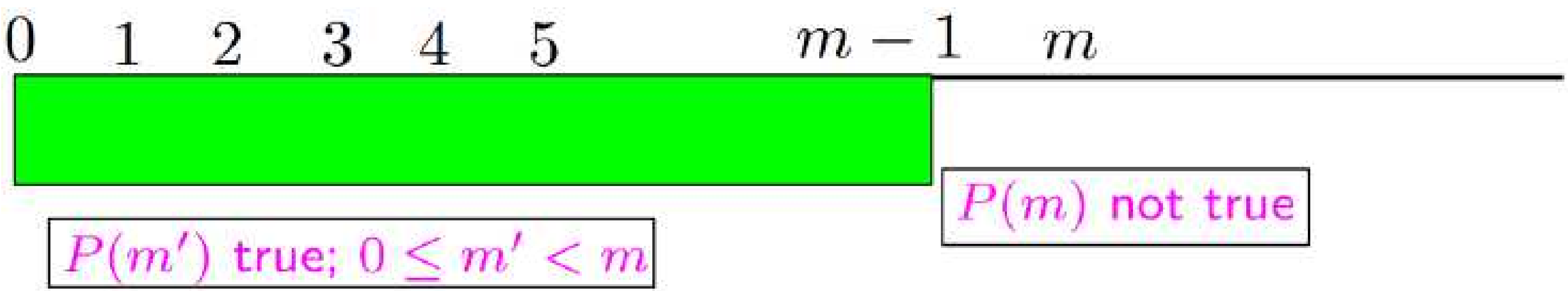
Proof by Smallest Counterexample

- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

  (ii) Let $m > 0$ be the smallest value for which $P(n)$ is false



Proof by Smallest Counterexample

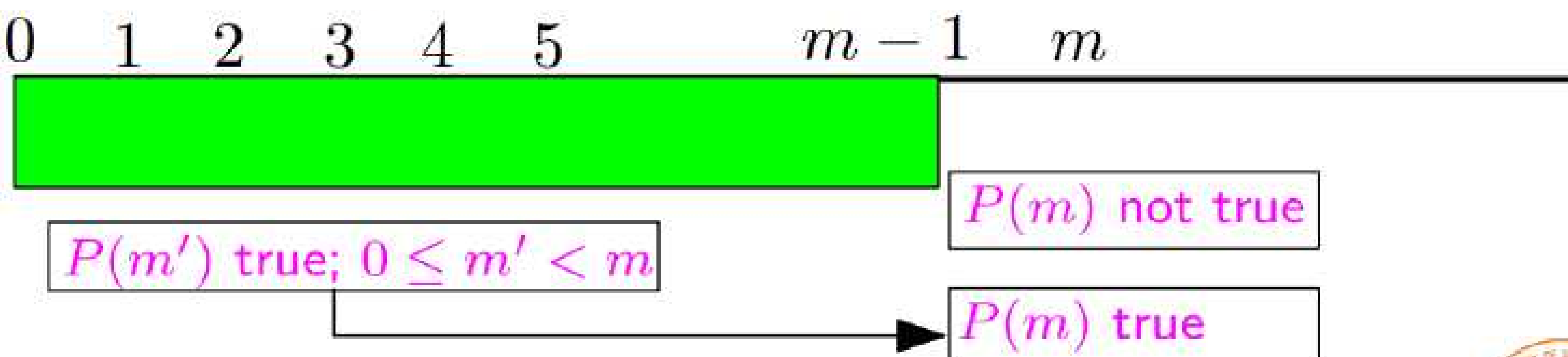
- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

  (ii) Let $m > 0$ be the smallest value for which $P(n)$ is false

  (iii) Then use the fact that $P(m')$ is true for all $0 \leq m' < m$ to show that $P(m)$ is true, contradicting the choice of m.



Proof by Smallest Counterexample

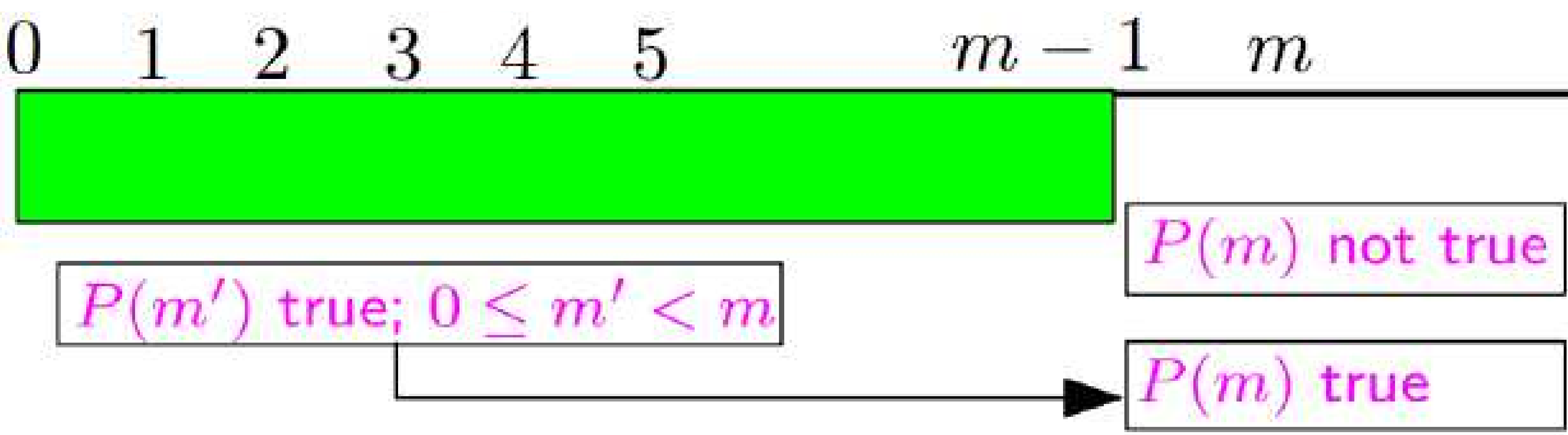
- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

  (ii) Let $m > 0$ be the smallest value for which $P(n)$ is false

  (iii) Then use the fact that $P(m')$ is true for all $0 \leq m' < m$ to show that $P(m)$ is true, contradicting the choice of m.



contradiction!

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

  - Suppose that $(*)$ is not always true

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

  - ◇ Suppose that $(*)$ is not always true
  - ◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0+1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

  ◇ Suppose that $(*)$ is not always true

  ◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

  ◇ For any nonnegative integer $i < n$,

$$1+2+\cdots+i=\frac{i(i+1)}{2}$$

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

◇ Suppose that $(*)$ is not always true

◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

◇ For any nonnegative integer $i < n$,

$$1 + 2 + \cdots + i = \frac{i(i+1)}{2}$$

◇ Since $0 = 0 \cdot 1/2$, $(*)$ holds for $n = 0$

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

◇ Suppose that $(*)$ is not always true

◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

◇ For any nonnegative integer $i < n$,

$$1 + 2 + \cdots + i = \frac{i(i+1)}{2}$$

◇ Since $0 = 0 \cdot 1/2$, $(*)$ holds for $n = 0$

◇ The smallest counterexample n is larger than 0

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  - Substituting $n-1$ for i gives
    $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  ◇ Substituting $n-1$ for i gives
  $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$

  ◇ Adding n to both sides gives
  $$1+2+\cdots+n-1+n=\frac{(n-1)n}{2}+n=\frac{n(n+1)}{2}$$

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  - ◇ Substituting $n-1$ for i gives
    $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$
  - ◇ Adding n to both sides gives
    $$1+2+\cdots+n-1+n=\frac{(n-1)n}{2}+n=\frac{n(n+1)}{2}$$
  - ◇ Thus, n is not a counterexample. Contradiction!

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  ◇ Substituting $n-1$ for i gives
  $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$

  ◇ Adding n to both sides gives
  $$1+2+\cdots+n-1+n=\frac{(n-1)n}{2}+n=\frac{n(n+1)}{2}$$

  ◇ Thus, n is not a counterexample. Contradiction!

  ◇ Therefore, $(*)$ holds for all positive integers n.

Example 1

- What implication did we have to prove?

Example 1

- What implication did we have to prove?

  The key step was proving that

$$P(n-1) \rightarrow P(n)$$

  where $P(n)$ is the statement

$$1+2+\cdots+n=\frac{n(n+1)}{2}$$

Example 2

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$2^{n+1} \geq n^2 + 2.$$

Example 2

- Use proof by smallest counterexample to show that, $\forall n \in N$,
$$2^{n+1} \geq n^2 + 2.$$

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$. We start by assuming that the statement

$$\forall n \in N \; P(n)$$

is false.

Example 2

- Use proof by smallest counterexample to show that, $\forall n \in N$,
$$2^{n+1} \geq n^2 + 2.$$

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$. We start by assuming that the statement

$$\forall n \in N \ P(n)$$

is false.

When a for all quantifier is false, there must be some n for which it is false. Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  This means that, for all $i \in N$ with $i < n$,
  $$2^{i+1} \geq i^2 + 2$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  This means that, for all $i \in N$ with $i < n$,

  $$2^{i+1} \geq i^2 + 2$$

  Since $2^{0+1} \geq 0^2 + 2$, we know that $n > 0$. Thus, $n - 1$ is a nonnegative integer less than n.

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  This means that, for all $i \in N$ with $i < n$,
  $$2^{i+1} \geq i^2 + 2$$

  Since $2^{0+1} \geq 0^2 + 2$, we know that $n > 0$. Thus, $n - 1$ is a nonnegative integer less than n.

  Then setting $i = n - 1$ gives
  $$2^{(n-1)+1} \geq (n-1)^2 + 2.$$

  or
  $$(*) \quad 2^n \geq n^2 - 2n + 1 + 2 = n^2 - 2n + 3$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\qquad (*)$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\qquad (*)$

  Multiply both sides by 2, giving

$$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\qquad (*)$

  Multiply both sides by 2, giving

  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

  To get a contradiction, we want to convert the right side into $n^2 + 2$ plus an additional nonnegative term.

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\quad (*)$

  Multiply both sides by 2, giving

  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

  To get a contradiction, we want to convert the right side into $n^2 + 2$ plus an additional nonnegative term.

  Thus, we write

  $$\begin{aligned} 2^{n+1} &\geq 2n^2 - 4n + 6 \\ &= (n^2 + 2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n-2)^2 \\ &\geq n^2 + 2. \end{aligned}$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\qquad (*)$

  Multiply both sides by 2, giving

  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

  To get a contradiction, we want to convert the right side into $n^2 + 2$ plus an additional nonnegative term.

  Thus, we write

  $$\begin{aligned} 2^{n+1} &\geq 2n^2 - 4n + 6 \\ &= (n^2 + 2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n - 2)^2 \\ \text{contradiction!} \quad &\geq n^2 + 2. \end{aligned}$$

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \to P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  - ◇ Suppose there is some n for which $P(n)$ is false $(*)$
  - ◇ Let n be the smallest counterexample
  - ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

  ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

  ◇ Therefore, from (b), using direct inference, $P(n)$ is true

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \to P(n)$

  - ◇ Suppose there is some n for which $P(n)$ is false $(*)$
  - ◇ Let n be the smallest counterexample
  - ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true
  - ◇ Therefore, from (b), using direct inference, $P(n)$ is true
  - ◇ This contradicts $(*)$.

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

  ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

  ◇ Therefore, from (b), using direct inference, $P(n)$ is true

  ◇ This contradicts $(*)$.

  ◇ Thus, $P(n)$ is true for all $n \in N$.

Example 2

- What did we really do?

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

Example 2

- What did we really do?

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  We then used proof by smallest counterexample to derive that $P(n)$ is true for all $n \in N$.

Example 2

- What did we really do?

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

We just showed that

(a) $P(0)$ is true

(b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

We then used proof by smallest counterexample to derive that $P(n)$ is true for all $n \in N$.

This is an *indirect proof*. Is it possible to prove this fact *directly*?

Example 2

- What did we really do?

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  We then used proof by smallest counterexample to derive that $P(n)$ is true for all $n \in N$.

  This is an *indirect proof*. Is it possible to prove this fact *directly*?

  Since $P(n-1) \rightarrow P(n)$, we see that

  $P(0)$ implies $P(1)$, $P(1)$ implies $P(2)$, ...

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

  This is actually **equivalent** to the *principle of mathematical induction*.

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

  This is actually **equivalent** to the *principle of mathematical induction*.

  Principle. (*the Weak Principle of Mathematical Induction*)

  (a) If the statement $P(b)$ is true

  (b) the statement $P(n-1) \rightarrow P(n)$ is true for all $n > b$, then $P(n)$ is true for all integers $n \geq b$

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

  This is actually **equivalent** to the *principle of mathematical induction*.

  Principle. (*the Weak Principle of Mathematical Induction*)
  (a) If the statement $P(b)$ is true
  (b) the statement $P(n-1) \rightarrow P(n)$ is true for all $n > b$,
  then $P(n)$ is true for all integers $n \geq b$

  (a) – *Basic Step* *Inductive Hypothesis*

  (b) – *Inductive Step* *Inductive Conclusion*

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

  (ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

(i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

(ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 4 \\ &= (n^2 + 2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n-2)^2 \\ &\geq n^2 + 2 \end{aligned}$$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

  (ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 4 \\ &= (n^2+2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n-2)^2 \\ &\geq n^2 + 2 \end{aligned}$$

  Hence, we've just prove that for $n > 0$, $P(n-1) \rightarrow P(n)$.

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

(i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

(ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 4 \\
&= (n^2+2) + (n^2 - 4n + 4) \\
&= n^2 + 2 + (n-2)^2 \\
&\geq n^2 + 2
\end{aligned}
$$

Hence, we've just prove that for $n > 0$, $P(n-1) \rightarrow P(n)$.

By mathematical induction, $\forall n > 0,\ 2^{n+1} \geq n^2 + 2$.

Proof by Induction

- $\forall n \geq 2$, $2^{n+1} \geq n^2 + 3$

Proof by Induction

- $\forall n \geq 2$, $2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 6 \\ &= n^2 + 3 + n^2 - 4n + 4 + 1 \\ &= n^2 + 3 + (n-2)^2 + 1 \\ &> n^2 + 3 \end{aligned}$$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 6 \\
&= n^2 + 3 + n^2 - 4n + 4 + 1 \\
&= n^2 + 3 + (n-2)^2 + 1 \\
&> n^2 + 3
\end{aligned}
$$

  Hence, we've just prove that for $n > 2$, $P(n-1) \rightarrow P(n)$.

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 6 \\
&= n^2 + 3 + n^2 - 4n + 4 + 1 \\
&= n^2 + 3 + (n-2)^2 + 1 \\
&> n^2 + 3
\end{aligned}
$$

  Hence, we've just prove that for $n > 2$, $P(n-1) \to P(n)$.

  By mathematical induction, $\forall n > 2,\ 2^{n+1} \geq n^2 + 3$.

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

Let $P(n)$ – $2^{n+1} \geq n^2 + 3$ Base Step

(i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

(ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3$ $\quad (*)$

Inductive Hypothesis

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 6 \\ &= n^2 + 3 + n^2 - 4n + 4 + 1 \\ &= n^2 + 3 + (n-2)^2 + 1 \\ &> n^2 + 3 \end{aligned}$$

Inductive Step

Hence, we've just prove that for $n > 2$, $P(n-1) \rightarrow P(n)$.

By mathematical induction, $\forall n > 2,\ 2^{n+1} \geq n^2 + 3$.

Inductive Conclusion

Another Form of Induction

- We may have another form of *direct proof* as follows.

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$
  - ◇ Next suppose that we have a proof that, $\forall k > 0$,

$$P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \rightarrow P(k)$$

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$
  - ◇ Next suppose that we have a proof that, $\forall k > 0$,

$$P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \rightarrow P(k)$$

  - ◇ Then, $P(0)$ implies $P(1)$

$P(0) \wedge P(1)$ implies $P(2)$

$P(0) \wedge P(1) \wedge P(2)$ implies $P(3)$ ...

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$
  - ◇ Next suppose that we have a proof that, $\forall k > 0$,

$$P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \rightarrow P(k)$$

  - ◇ Then, $P(0)$ implies $P(1)$

$P(0) \wedge P(1)$ implies $P(2)$

$P(0) \wedge P(1) \wedge P(2)$ implies $P(3)$ ...

  - ◇ Iterating gives us a proof of $P(n)$ for all n

Strong Induction

- **Principle** (*The Strong Principle of Mathematical Induction*)

  (a) If the statement $P(b)$ is true

  (b) for all $n > b$, the statement
  $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$ is true.

  then $P(n)$ is true for all integers $n \geq b$.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.
  - ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

  ◇ Then, if n is not a prime power, it is a product of two smaller numbers, each of which is, by the inductive hypothesis, a power of a prime or a product of powers of primes.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

  ◇ Then, if n is not a prime power, it is a product of two smaller numbers, each of which is, by the inductive hypothesis, a power of a prime or a product of powers of primes.

  ◇ Thus, by the strong principle of mathematical induction, every positive integer is a power of a prime or a product of powers of primes.

Mathematical Induction

- In practice, we do not usually explicitly distinguish between the weak and strong forms.

- In practice, we do not usually explicitly distinguish between the weak and strong forms.

- In reality, they are equivalent to each other in that the weak form is a special case of the strong form, and the strong form can be derived from the weak form.

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step
  2. We then, $\forall n > b$, show either

$$(*) \qquad P(n-1) \rightarrow P(n)$$

or

$$(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$$

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step
  2. We then, $\forall n > b$, show either

$$(*) \qquad P(n-1) \rightarrow P(n)$$

or

$$(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$$

  We need to make the inductive hypothesis of either $P(n-1)$ or $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1)$.We then use $(*)$ or $(**)$ to derive $P(n)$.

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

1. We show that $P(b)$ is true. – Base Step
2. We then, $\forall n > b$, show either

$$(*) \qquad P(n-1) \rightarrow P(n)$$

or

$$(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$$

   We need to make the inductive hypothesis of either $P(n-1)$ or $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1)$.We then use $(*)$ or $(**)$ to derive $P(n)$.

3. We conclude on the basis of the principle of mathematical induction that $P(n)$ is true for all $n \geq b$.

Next Lecture

- recurrence ...