Computer and Network Security: Modern Cryptography Overview

Kameswari Chebrolu

Some figures/text taken from wikipedia.com

Outline

- **Modern Cryptography**
  - **Overview**
  - Confidentiality
    - Crypto-analysis, One Time Pads
    - Symmetric key encryption, Block modes
    - Asymmetric key encryption
  - Integrity (includes Authentication)
    - Hashes, MAC, Digital signature

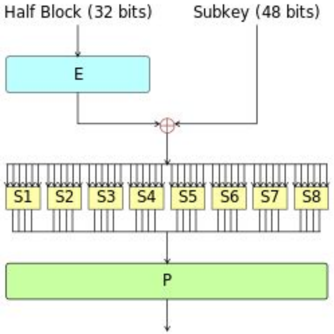
Overview Outline

- **Classic vs Modern Cryptography**
- History
- Goals of Modern Cryptography

Cryptography

- Crypto: Hidden/Secret; Graphy: Writing
- Secure communication in presence of adversaries
  - Practiced by cryptographers

Classical vs Modern



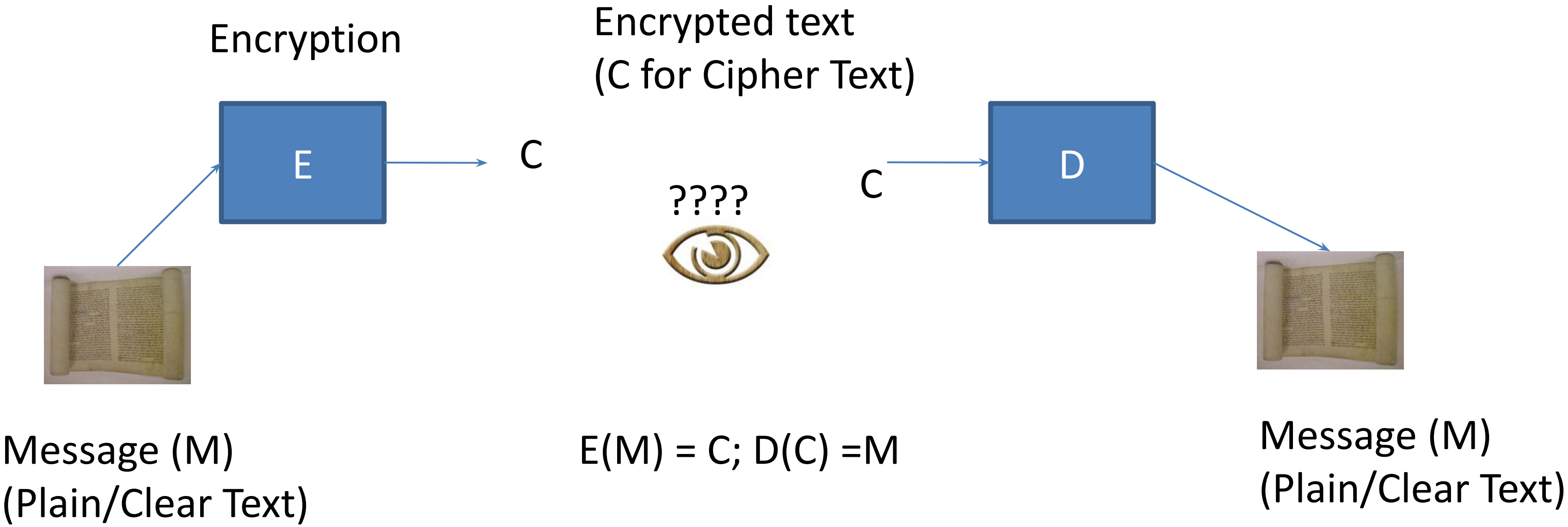
Classical

- **Confidentiality**
- Plain text
- Military
- Secrecy of protocol/algorithm

Modern

- **Confidentiality**, Integrity
  - Further digital cash, secure voting etc
- Deals with bits
- Every one
- Provable security based on mathematics (protocol /algorithm often open)

Confidentiality Set-up



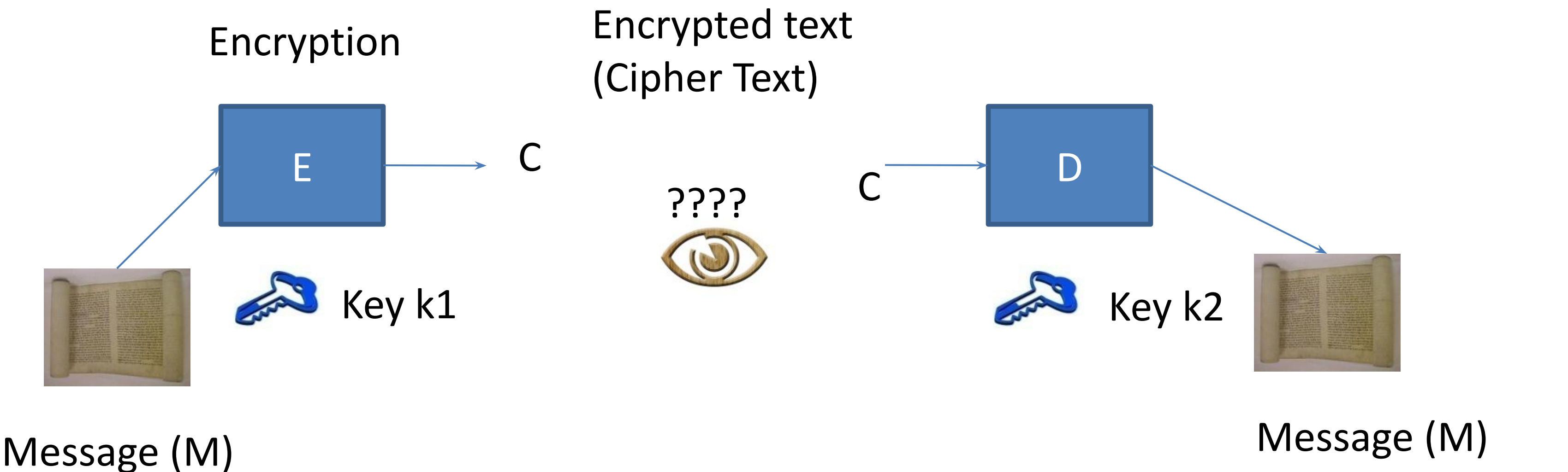
$E(M) = C; D(C) = M$

Cipher/Cryptographic Algorithm: Mathematical function used for encryption and decryption

Classical Cryptography

- Restricted algorithm
  - Keep the algorithm secret
  - Not used today. Why?
    - Difficult to manage churn in group
      - More scope for accidental leaks
    - No quality control
    - Cannot use off-the-shelf hardware or software

Updated Set-up



$E_{k1}(M) = C; D_{k2}(C) = M$

Algorithm public, Key secret

Modern Cryptography

- Works with bits instead of alphabet
- Introduces the notion of key
  - Key: one of a large number of values
  - Keyspace: Range of possible keys
  - Security is based on key, not algorithm

Modern Cryptography

- Based on complex mathematics and/or combines elements of substitution and transposition
  - Focuses on provable security
- Advantages:
  - Algorithm analyzed by world's best cryptographers
  - Mass production

Outline

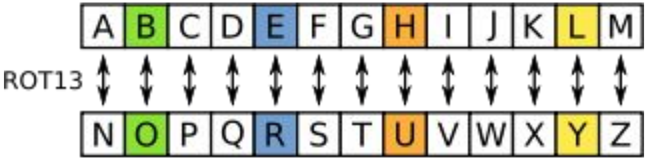
- Classic vs Modern Cryptography
- **History**
- Goals of Modern Cryptography

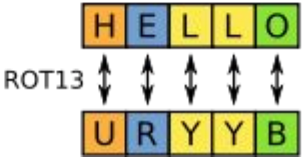
History

- Cryptography usage dates to ~ 1500 BCE
- Substitution Ciphers (500BCE) □ Transposition Ciphers (3BCE)□ Polyalphabetic Ciphers (1500s) □ Mechanization (1800s)□ Modern Cryptography (1950+)
- Predominantly military use □ Everyday use
- Confidentiality □ Much more (Integrity , anonymity, digital cash etc)

Substitution Cipher

- Replace a character with another
- Algorithm: Monoalphabetic cipher
- Key: substitution table
- How strong?
  - Brute Force (26! Combinations, 4 * 10^{26})
  - Very large key space but not very strong. Why?
  - Susceptible to frequency analysis





ROT13: Caesar cipher (alphabet rotated by 13 steps)

Use: Online forums for hiding spoilers, puzzle solutions etc

Grasping Large Numbers

Number	
9.46×10^{15}	Distance (in metres) travelled by light in one year (1 light year or 9.46 trillion kilometres).
4.32×10^{17}	Estimated age (in seconds) of the universe (assuming 13.7 billion years since the Big Bang).
8.8×10^{26}	Approximate diameter (in metres) of the visible universe (93 billion light years).
3×10^{52}	Estimated mass (in kilograms) of the observable universe.
1×10^{80}	Estimate the total number of fundamental particles in the observable universe (other estimates go up to 10^{85}).

From:
http://www.physicsoftheuniverse.com/numbers.html

Frequency Analysis

```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIM
WQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITREWHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJ
GSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXV
IZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQMXLE
PPXLIECCIEVEWGISJKTVWMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPP
XLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX
```

- I most common single letter
- XL most common bigram
- XLI most common trigram
- E second most common letter
- ‘e’ most common in English
- ‘th’ most common bigram
- ‘the’ most common trigram
- ‘a’ second most common in English

Strongly suggests X~t, L~h, I~e and E~a

```
heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVSTYhtZetheKeetPeJVSZaYPaRRGaReM
WQhMGhMtQaReWGPSReHMtQaRaKeaTtMJTPRGaVaKaeTRaWHatthattMZeTWAWSQWtSWatTVaPMRtRSJ
GSTVReaYVeatCVMUeMWaRGMeWtMJMGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtV
eZMtFSJtheKaGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWHYPSRRFQMtha
PPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQeMYhtSJtheMWReGtQaROeVFVeZaVAaKPeaWHtaAMWYaPP
thMWYRMWtSGSWRMHeVatMSWMGSTPHhaVHPFKPaZeNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt
```

Rtate --> State (R~s)

atthattMZe --> at that time (M~i and Z~m)

and so on.....

Other Types

- Make frequency analysis difficult
- Goal: Flatten frequency distribution
- Homophonic Substitution Cipher (1400CE)
  - A character can map to one of several characters of ciphertext
    - Ciphertext alphabet larger than plaintext alphabet
    - Ciphertext alphabet can be numeric or upper/lower case or whole new alphabet
    - E.g. A can map to 12 or 34 or 45 or 77; B can map to 6 or 64;

- Polygram substitution cipher (1850CE): Blocks of characters are encrypted in groups
  - E.g. THE □ ABC; ORA □ LMB

History

- Cryptography usage dates to ~ 1500 BCE
- Substitution Ciphers (500BCE) □ Transposition Ciphers (3BCE)□ Polyalphabetic Ciphers (1500s) □ Mechanization (1800s)□ Modern Cryptography (1950+)
- Predominantly military use □ Everyday use
- Confidentiality □ Much more (Integrity , anonymity, digital cash etc)

Polyalphabetic Cipher (1568CE)

- Made up of multiple mono-alpabetic ciphers
- Key decides which cipher to use
  - Keys recycled after use
  - Key length: period of cipher
- E.g. Vigenere Cipher

Example: Vigenère cipher (1553CE)

Plaintext:ATTACKATDAWN

Key:LEMONLEMONLE

Ciphertext:LXFOPVEFRNHR

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

Polyalphabetic Cipher (1568CE)

- Running-key or Book Cipher: Key can be a book or long poem
- Seed of Modern Cryptography
  - Make key as long and unpredictable as possible

Running Key Cipher

- Page 63, line 1 is selected as the running key:

“errors can occur in several places. A label has….”

Plaintext:	f l e e a t o n c e w e a r e d i s c o v e r e d
Running key:	E R R O R S C A N O C C U R I N S E V E R A L P L
Ciphertext:	J C V S R L Q N P S Y G U I M Q A W X S M E C T O

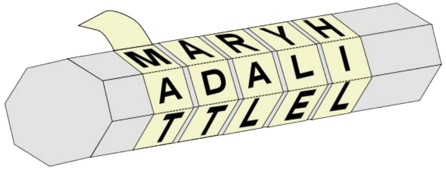
Indicator block specifies key: 3 characters for page , 2 for line number
Encoding: A=0, B=1 etc □ {06301 maps to AGDAB}
Final message: JCVSR LQNPS YGUIM QAWXS AGDAB MECTO

History

- Cryptography usage dates to ~ 1500 BCE
- Substitution Ciphers (500BCE) □ Transposition Ciphers (3BCE)□ Polyalphabetic Ciphers (1500s) □ Mechanization (1800s)□ Modern Cryptography (1950+)
- Predominantly military use □ Everyday use
- Confidentiality □ Much more (Integrity , anonymity, digital cash etc)

Transposition Cipher

- Same letters but order shuffled
- Example:
  - Message: WE ARE DISCOVERED. FLEE AT ONCE.
  - Key: ZEBRAS (632415; alphabetical order)
  - Cipher text: EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
- Double transposition increases security even further
- Shortcoming: Requires memory



Scytale (used by Greeks/Spartans)
"mary had a little lamb"

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

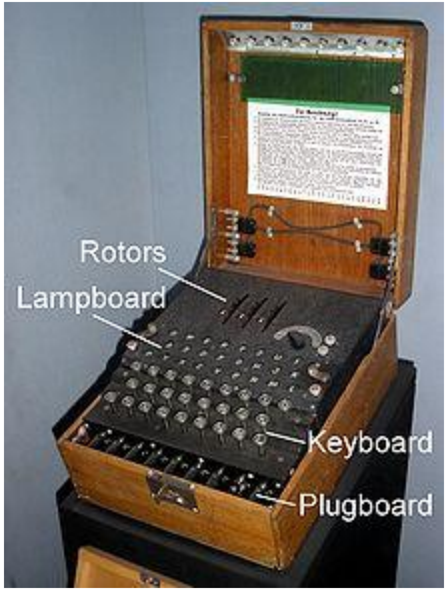
Null characters

History

- Cryptography usage dates to ~ 1500 BCE
- Substitution Ciphers (500BCE) Transposition Ciphers (3BCE) Polyalphabetic Ciphers (1500s) Mechanization (1800s) Modern Cryptography (1950+)
- Predominantly military use Everyday use
- Confidentiality Much more (Integrity , anonymity, digital cash etc)

Mechanization: Rotor machines

- Automate the process of encryption and decryption
- Rotor machine: series of rotors that implement a version of Vigenere cipher
- Example: Enigma used by Germans in WWII; broken by Polish cryptographers



German Enigma Machine

Outline

- Classic vs Modern Cryptography
- History
- **Goals of Modern Cryptography**

Modern Cryptography Goals

- **Confidentiality (Encryption)**
  - Symmetric key
  - Asymmetric key
- **Integrity (includes authentication)**
  - Hashes (message)
  - MACs (message/source identity)
  - Digital signature (message/source identity)
- Other areas
  - Currency, voting systems, anonymity etc

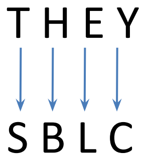
Crypto Cipher Examples

- Data Encryption Standard (DES), Advanced Encryption Standard (AES): Popular symmetric key algorithms
  - Used for encryption, MAC
- Rivest, Shamir, Adleman (RSA): Popular public-key algorithm
  - Used for encryption and digital signatures
- Digital Signature Algorithm (DSA): Public key algorithm
  - Cannot be used for encryption, only digital signatures
- SHA-1, SHA-2, SHA-3, MD4, MD5: Popular Hash functions
  - Only SHA-2 and SHA-3 safe currently

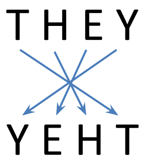
Building Block-1: Confusion and Diffusion

- Applicable to symmetric key algorithms
  - Encryption (confidentiality) and MACs (authentication + integrity)

- Confusion: Transform information in plaintext so that it is not easy to extract
  - Hide plaintext symbols
  - Achieved by substitution



- Diffusion: Spread information from a region of plaintext much wider in cipher text
  - Achieved by transposition



- Symmetric ciphers use a combination of both

Building Block-2: One Way Functions

- Applicable to hashes (integrity)
- Applicable to asymmetric key algorithms
  - Encryption (confidentiality), Digital signatures (integrity + authentication)

One Way Functions

- Easy to compute but difficult to invert (hashes)
- One way functions with trapdoor: Easy to invert but with a key (asymmetric key algo.)
- Example:
  - Easy to multiple two large primes p1 * p2
  - Difficult to factor (p1*p2) to recover p1 and p2
  - Given (p1*p2) and p1; easy to recover p2

Background: Computational Complexity

- Algorithms classified according to time and space complexity; n is the input size
- Focus: Time complexity
  - E.g. $n^2 + 12n + 5$ □ $O(n^2)$
- Different classes of algorithms
  - Constant: $O(1)$ (independent of n)
  - Polynomial: $O(n^m)$, m is a constant
  - Exponential: $O(c^{f(n)})$
    - c is a constant > 1 and f(n) polynomial function in n

Complexity of Problems

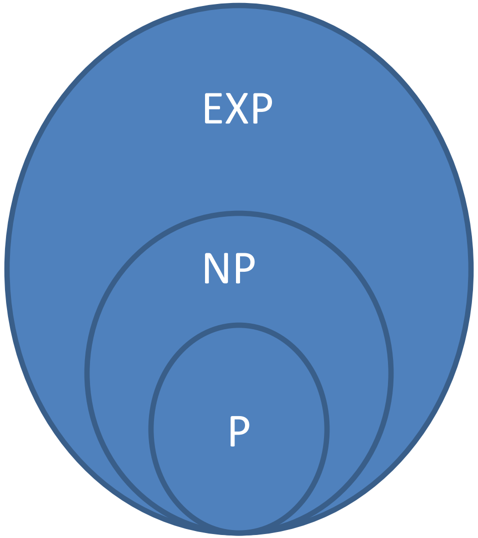
- Characterize complexity of a problem, not just a particular algorithm to solve the problem
- Minimum time required to solve problem on a turing machine
  - Machine with finite state but infinite read-write memory tape
- Nondeterministic turing machine: A machine that can make guesses and check the guess in polynomial time

Complexity Classes

- P: Solvable in polynomial time (e.g. sorting a list)
  - verifying solution also polynomial
- NP: Solvable in polynomial time on a non-deterministic turing machine(e.g. traveling salesman problem)
  - Can verify solution in polynomial time
  - Finding solution may not be polynomial
    - Polynomial if machine can guess the solution or try all guesses in parallel

Complexity Classes

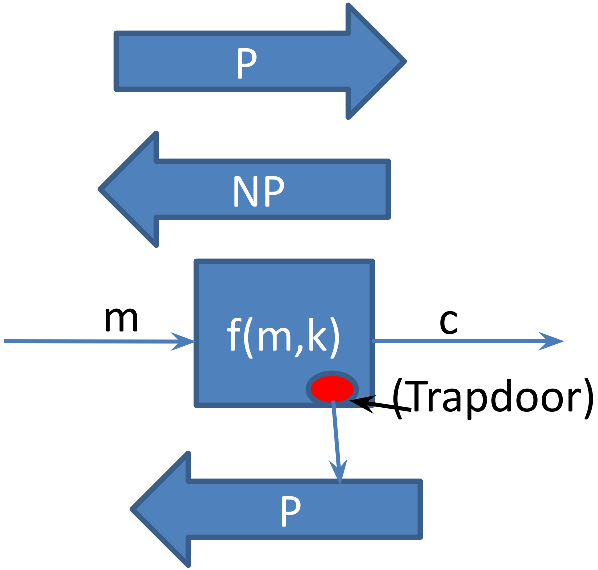
- NP-complete: Hardest problems in NP
  - If *any NP-complete problem* can be solved in polynomial time, then *every problem in NP* can also be solved
- EXP: solvable in exponential time
  - verifying solution may not be polynomial
- Is P = NP? Open question



Relevance to Cryptography

- Focus on encryption
- Attacker has to solve an NP complete problem to recover plain text
- NP complete problem examples:
  - Integer factorization: Find the prime factors of number n
  - Discrete logarithm: Find x where $a^x = b$ (mod n)

  (deal with very large numbers, thousands of bits)



One way functions with trapdoor

$f(m,k)$ □ c (P)
$f^{-1}(c)$□ m (NP)
$f^{-1}(c,k)$□ m (P)

- Elliptic curve: Uses elliptic curves over finite fields

Summary

- Modern crypto more rigorous and achieves lot more than classical crypto
- Provides confidentiality and integrity (and much more)
- Goals achieved via symmetric, asymmetric key algorithms and hashes
- Building blocks:
  - Confusion and Diffusion
  - One-way functions (with trapdoors)
    - Based on computationally hard NP complete problems