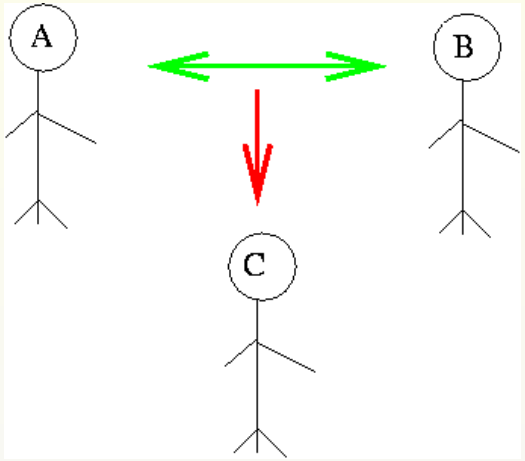
Cryptographic Protocols and Network Security

G. Sivakumar

Computer Science and Engineering
IIT Bombay
siva@iitb.ac.in

Oct 14, 2004

Exchanging Secrets



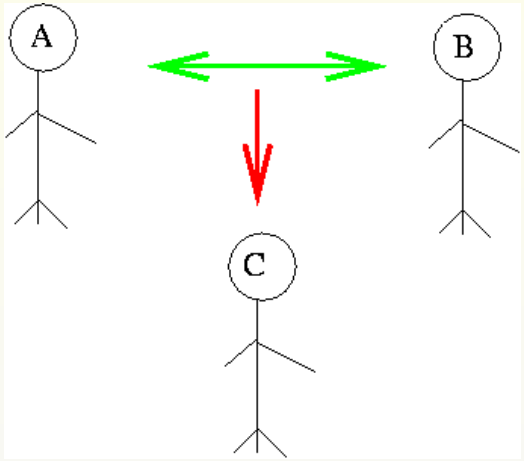
Goal

A and B to agree on a secret number. But, C can listen to all their conversation.

Solution?

A tells B: *I'll send you 3 numbers. Let's use their LCM as the key.*

Exchanging Secrets



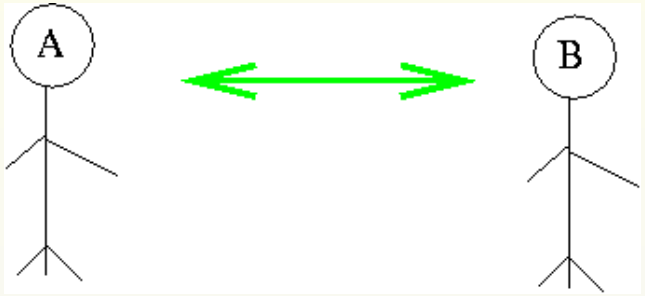
Goal

A and B to agree on a secret number. But, C can listen to all their conversation.

Solution?

A tells B: *I'll send you 3 numbers. Let's use their LCM as the key.*

Mutual Authentication



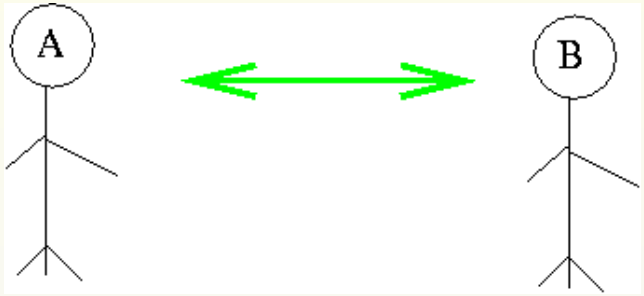
Goal

A and B to verify that both know the same secret number. No *third party* (intruder or umpire!)

Solution?

A tells B: *I'll tell you first 2 digits, you tell me the last two...*

Mutual Authentication



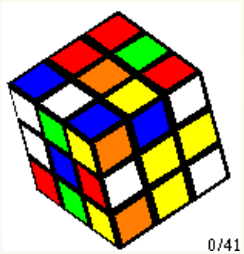
Goal

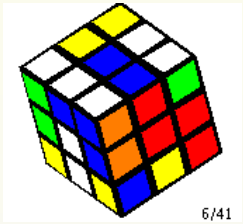
A and B to verify that both know the same secret number. No *third party* (intruder or umpire!)

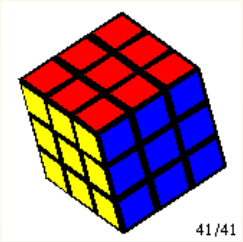
Solution?

A tells B: *I'll tell you first 2 digits, you tell me the last two...*

Zero-Knowledge Proofs







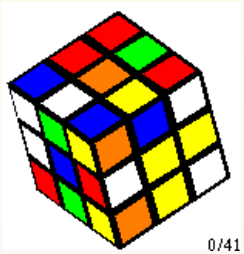
Goal

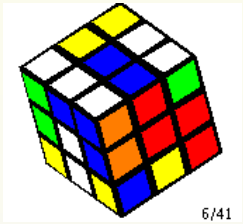
A to prove to B that she knows how to solve the cube. Without *actually revealing* the solution!

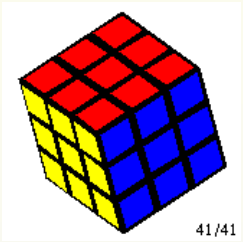
Solution?

A tells B: *Close your eyes, let me solve it...*

Zero-Knowledge Proofs







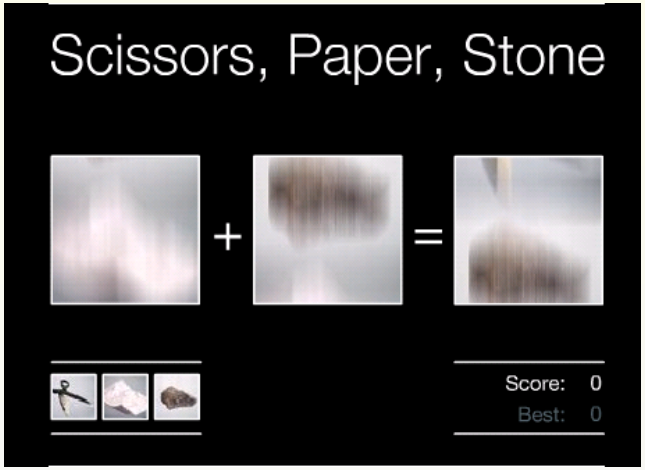
Goal

A to prove to B that she knows how to solve the cube. Without *actually revealing* the solution!

Solution?

A tells B: *Close your eyes, let me solve it...*

Paper, Scissors, Rock Game



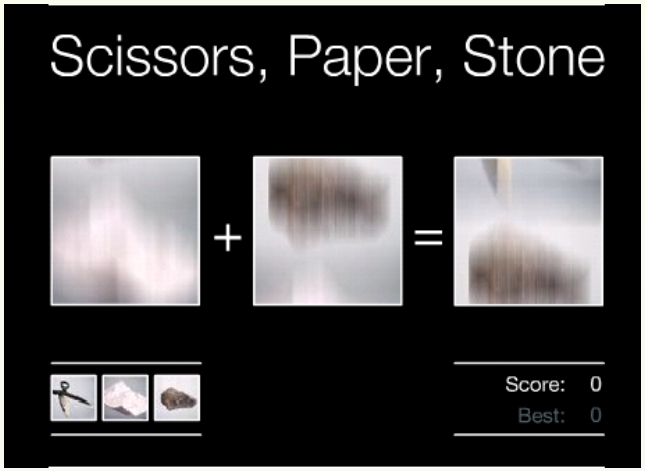
Goal

How to play over Internet? Using **email,** say?

Solution?

You mail me your choice. I'll reply with mine.

Paper, Scissors, Rock Game



Goal

How to play over Internet? Using **email,** say?

Solution?

You mail me your choice. I'll reply with mine.

Mr. Sum and Mr. Product

Someone thinks of two numbers between 2 and 500 inclusive. He then adds them up and whispers the sum to Mr. Sum. He also multiplies them together and whispers the product to Mr. Product. The following conversation then ensues.

- Mr Product: I don't know what the two original numbers were.
- Mr Sum: I already knew that you didn't know.
- Mr Product: Well now I know.
- Mr Sum: Aha! So do I.

What were the original two numbers?

Mr. Sum and Mr. Product

Someone thinks of two numbers between 2 and 500 inclusive. He then adds them up and whispers the sum to Mr. Sum. He also multiplies them together and whispers the product to Mr. Product. The following conversation then ensues.

- Mr Product: I don't know what the two original numbers were.
- Mr Sum: I already knew that you didn't know.
- Mr Product: Well now I know.
- Mr Sum: Aha! So do I.

What were the original two numbers?

Mr. Sum and Mr. Product

Someone thinks of two numbers between 2 and 500 inclusive. He then adds them up and whispers the sum to Mr. Sum. He also multiplies them together and whispers the product to Mr. Product. The following conversation then ensues.

- Mr Product: I don't know what the two original numbers were.
- Mr Sum: I already knew that you didn't know.
- Mr Product: Well now I know.
- Mr Sum: Aha! So do I.

What were the original two numbers?

Mr. Sum and Mr. Product

Someone thinks of two numbers between 2 and 500 inclusive. He then adds them up and whispers the sum to Mr. Sum. He also multiplies them together and whispers the product to Mr. Product. The following conversation then ensues.

- Mr Product: I don't know what the two original numbers were.
- Mr Sum: I already knew that you didn't know.
- Mr Product: Well now I know.
- Mr Sum: Aha! So do I.

What were the original two numbers?

Sharing a Dosa

Goal

All should get equal share of dosa. No *envy* factor. No *trusted umpire*.

Solution?

2 people case is easy- *you cut, i choose!*

Sharing a Dosa

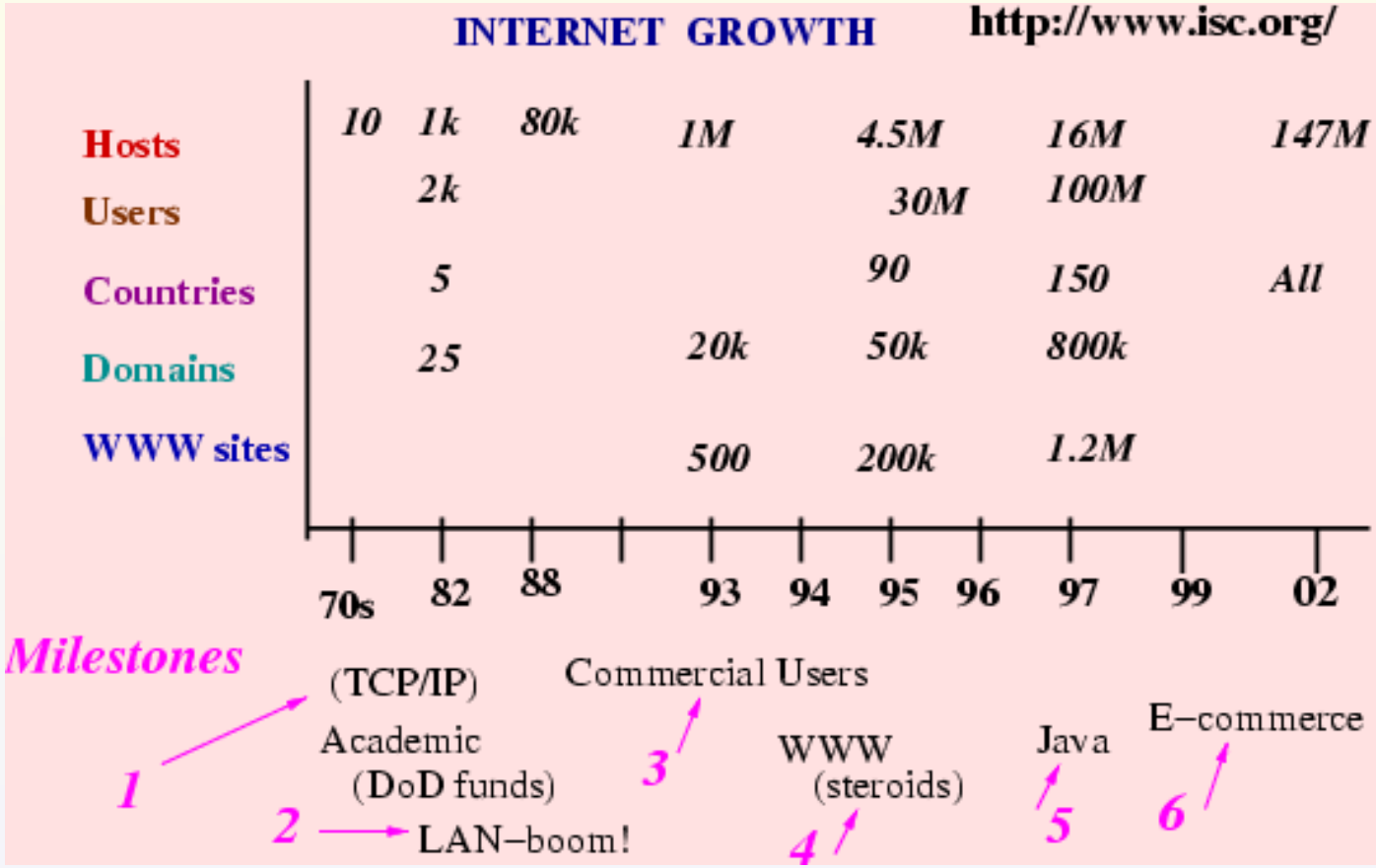
Goal

All should get equal share of dosa. No *envy* factor. No *trusted umpire*.

Solution?

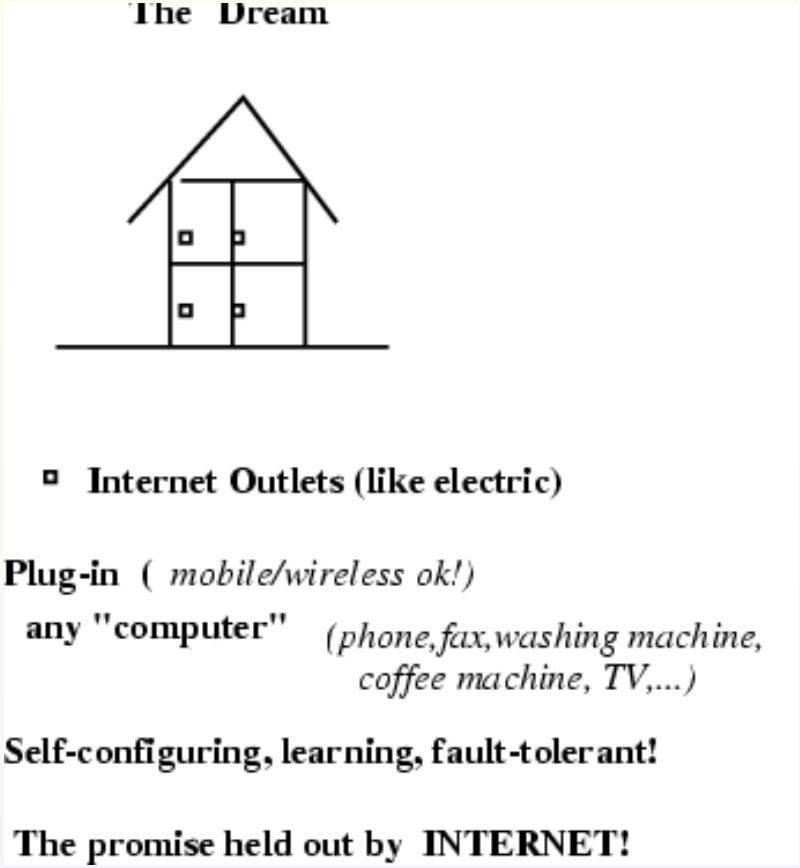
2 people case is easy- *you cut, i choose!*

Internet's Growth and Charter



Information **AnyTime, AnyWhere, AnyForm, AnyDevice, ...**
WebTone like DialTone

Internet's Dream



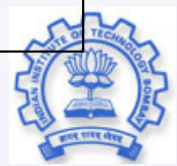
- Why should a fridge be on Internet?
- Will **security** considerations make this a **nightmare**?

Security Concerns

Match the following!

Problems	Attackers
Highly contagious viruses	Unintended blunders
Defacing web pages	Disgruntled employees or customers
Credit card number theft	Organized crime
On-line scams	Foreign espionage agents
Intellectual property theft	Hackers driven by technical challenge
Wiping out data	Petty criminals
Denial of service	Organized terror groups
Spam E-mails	Information warfare
Reading private files	...
Surveillance	...

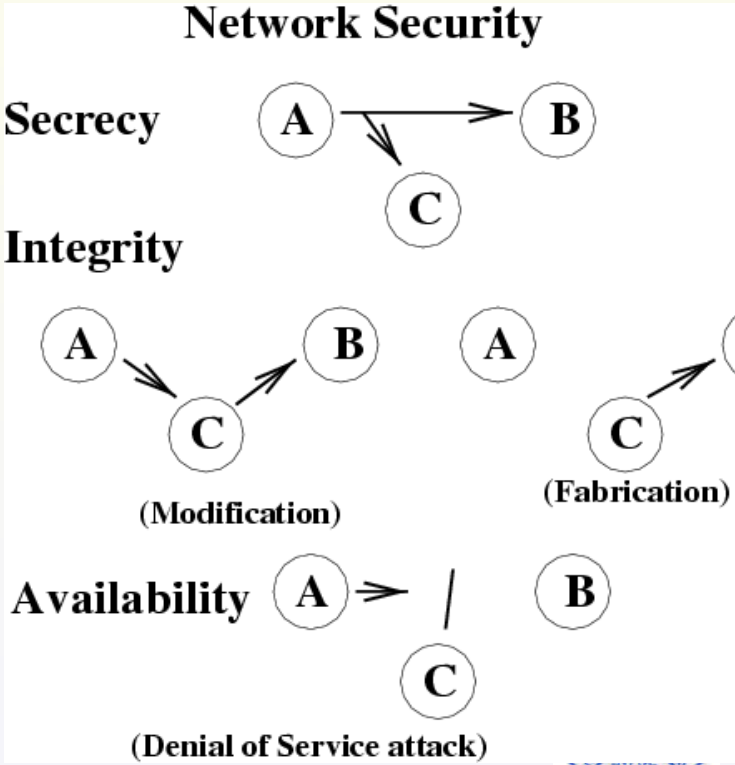
- Crackers vs. Hackers
- Note how much resources available to attackers.



Vulnerabilities

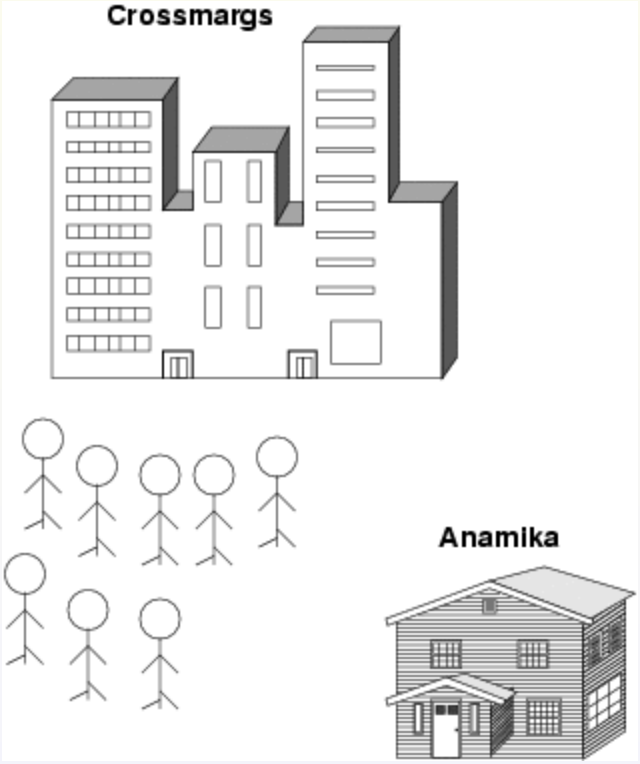
- **Application Security**
  - Buggy code
  - Buffer Overflows
- **Host Security**
  - Server side (multi-user/application)
  - Client side (virus)

Transmission Security

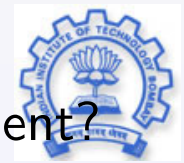


Denial of Service

Small shop-owner versus Supermarket

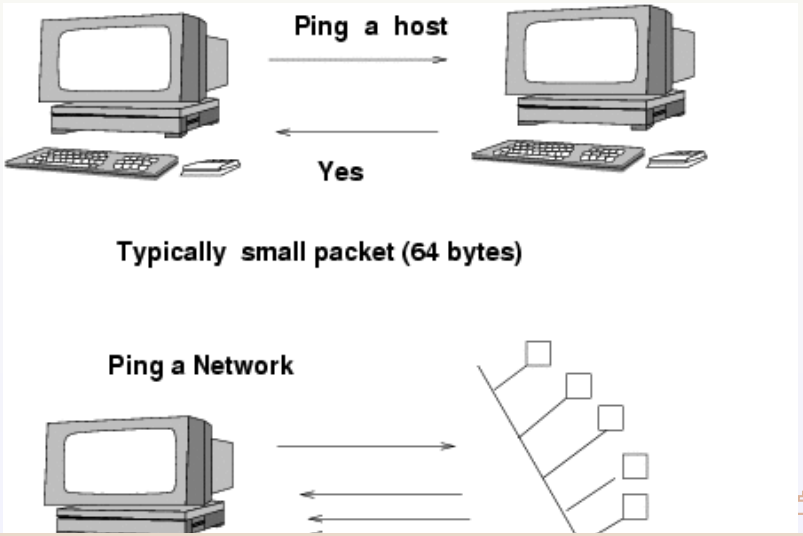


- What can the attacker do?
- What has he gained or compromised?
- What defence mechanisms are possible?
  - Screening visitors using guards (who looks respectable?)
  - VVIP security, but do you want to be isolated?
- what is the Internet equivalent?

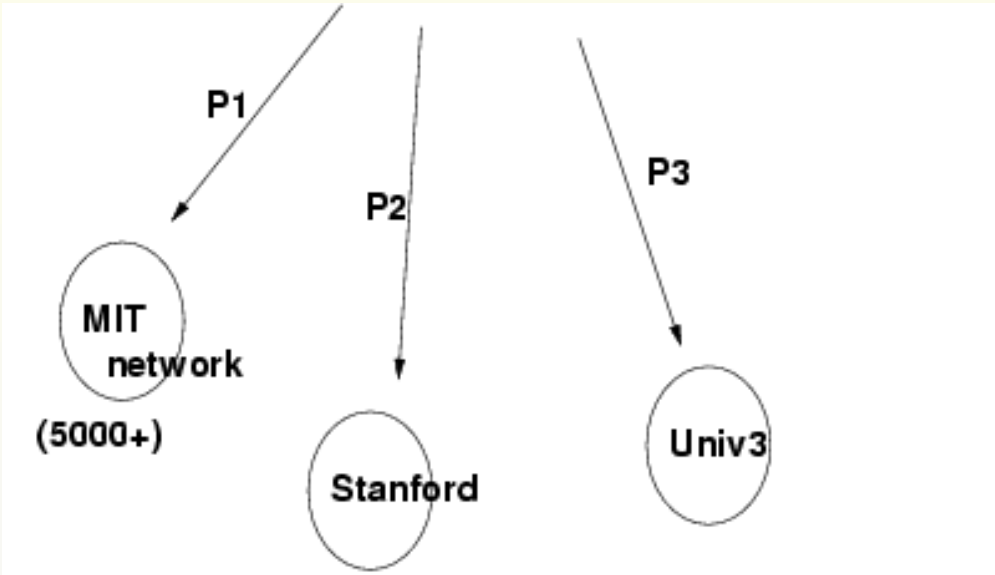


Yahoo DDoS attack

- A real example of network insecurity.
- Caused traffic to Yahoo to zoom to 100s of Mbps
- Broke the capacity of machines at Yahoo and its ISPs
- Internet Control Message Protocol (ICMP) normally used for good purposes.
- Ping used to check "are you alive?"



Yahoo DDoS attack



P1,P2,P3,... Fake broadcast ping from Victim

How many replies does unsupecting victim get?

From whom? (respectable?)

DDOS (distributed denial of service attack)

Freely available for "script kiddies" to wreak havoc!

Security Requirements

Informal statements (formal is much harder)

- Confidentiality Protection from disclosure to unauthorized persons
- Integrity Assurance that information has not been modified unauthorizedly.
- Authentication Assurance of identity of originator of information.
- Non-Repudiation Originator cannot deny sending the message.
- Availability Not able to use system or communicate when desired.
- Anonymity/Pseudonomity For applications like voting, instructor evaluation.
- Traffic Analysis Should not even know who is communicating with whom. Why?
- Emerging Applications Online Voting, Auctions (more later)

And all this with postcards (IP datagrams)!

Security Mechanisms

- **System Security:** "Nothing bad happens to my computers and equipment"
  virus, trojan-horse, logic/time-bombs, ...
- **Network Security:**
  - **Authentication Mechanisms** "you are who you say you are"
  - **Access Control** Firewalls, Proxies "who can do what"
- **Data Security:** "for your eyes only"
  - Encryption, Digests, Signatures, ...

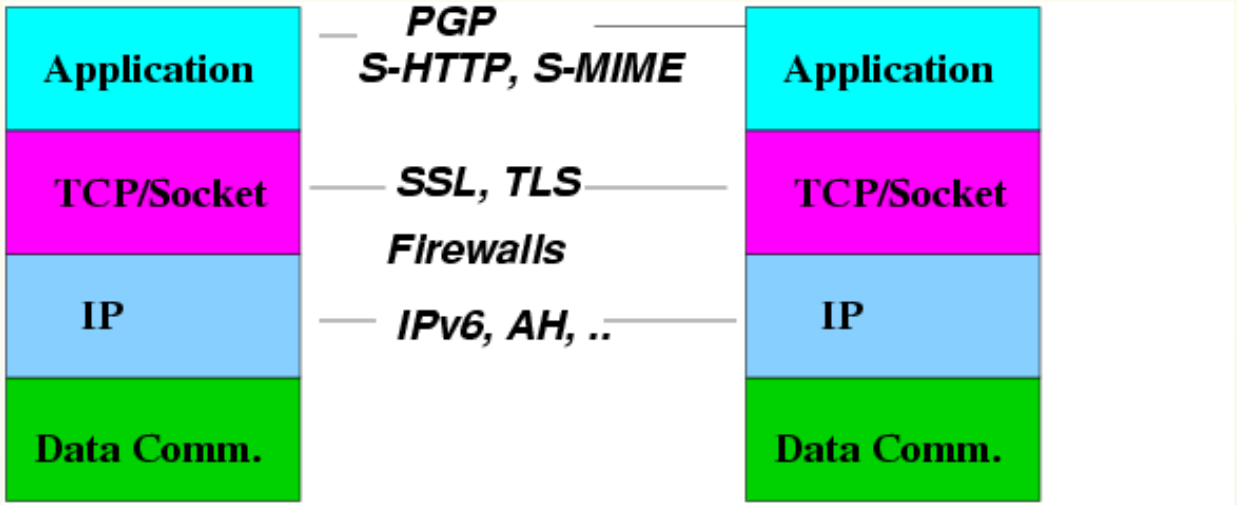
Security Mechanisms

- **System Security:** "Nothing bad happens to my computers and equipment"
  virus, trojan-horse, logic/time-bombs, ...
- **Network Security:**
  - **Authentication Mechanisms** "you are who you say you are"
  - **Access Control** Firewalls, Proxies "who can do what"
- **Data Security:** "for your eyes only"
  - Encryption, Digests, Signatures, ...

Security Mechanisms

- **System Security:** "Nothing bad happens to my computers and equipment"
  virus, trojan-horse, logic/time-bombs, ...
- **Network Security:**
  - **Authentication Mechanisms** "you are who you say you are"
  - **Access Control** Firewalls, Proxies "who can do what"
- **Data Security:** "for your eyes only"
  - Encryption, Digests, Signatures, ...

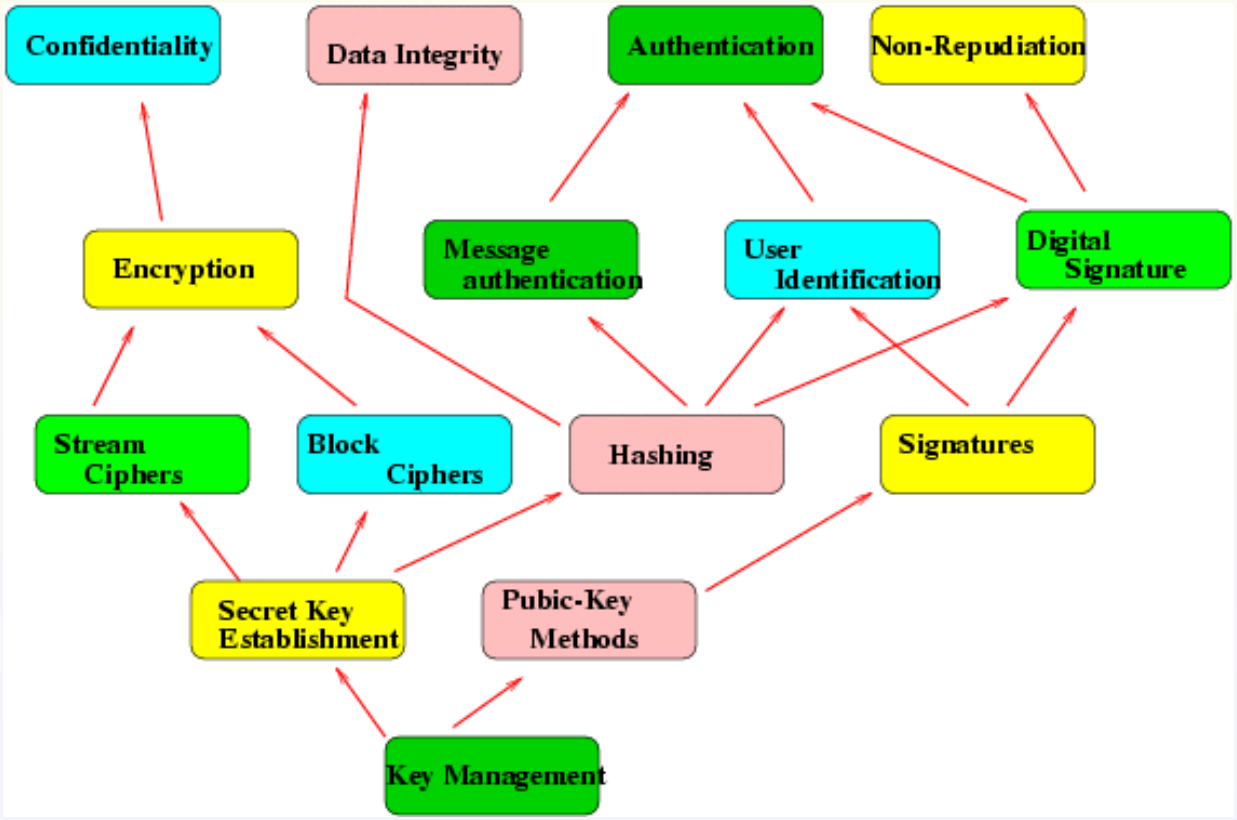
Network Security Mechanism Layers



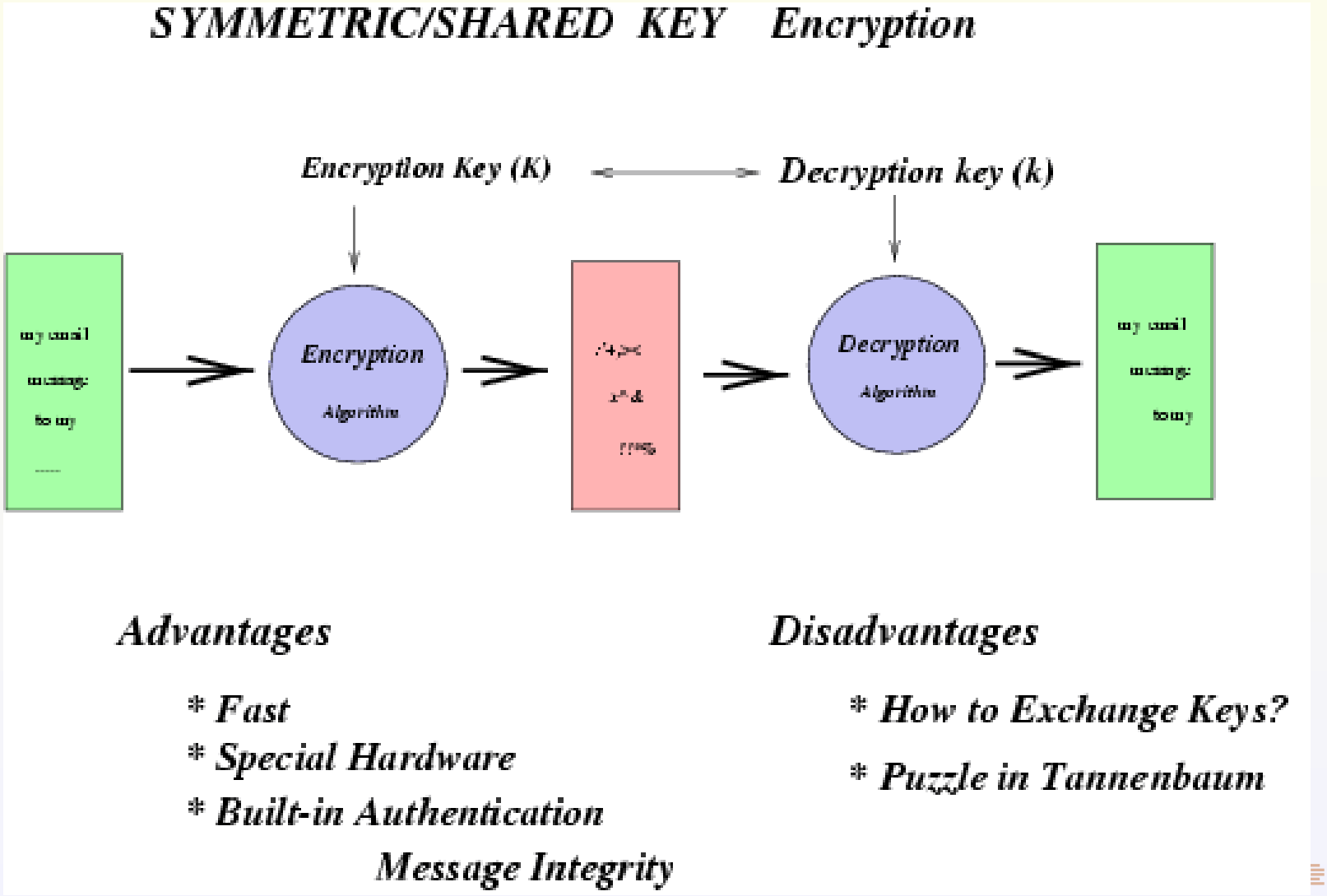
Cryptograhphic Protocols underly all security mechanisms. Real Challenge to design good ones for *key establishment*, *mutual authentication* etc.

Cryptography and Data Security

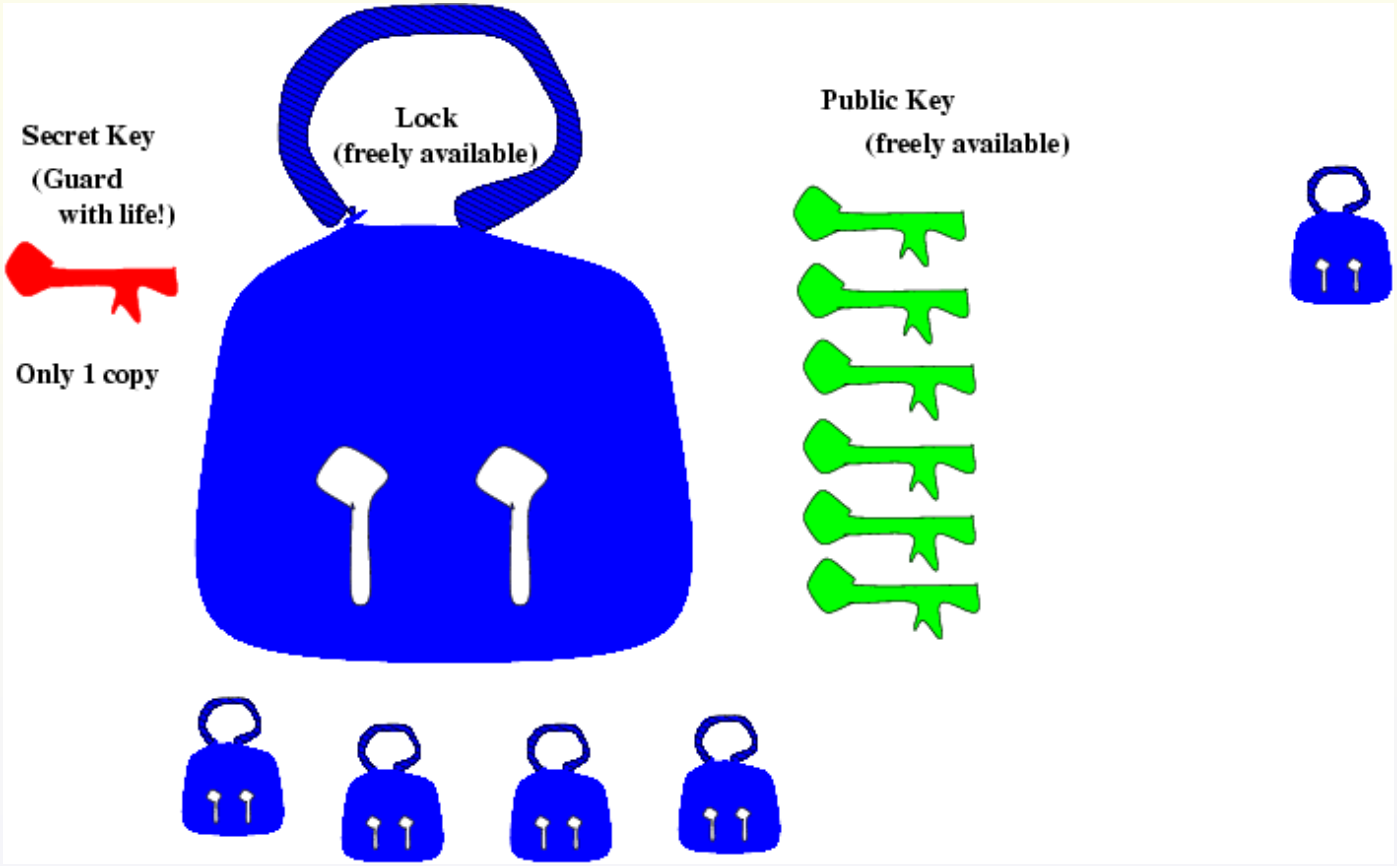
- *sine qua non* [without this nothing :-]
- Historically who used first? (L & M)
- Code Language in joint families!



Symmetric/Private-Key Algorithms

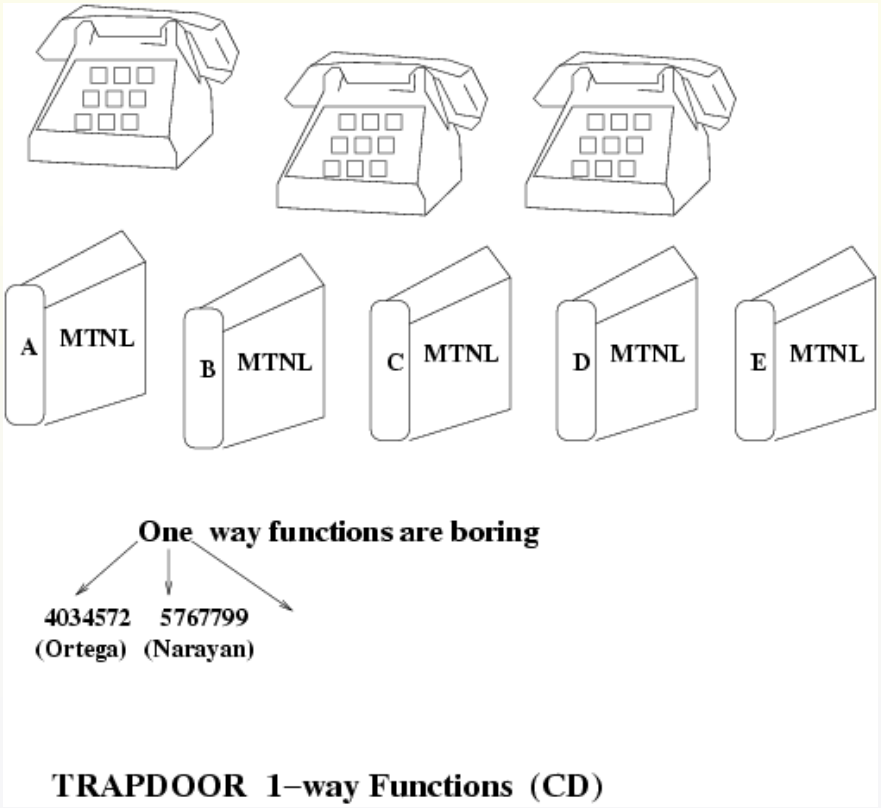


Asymmetric/Public-Key Algorithms



- Keys are duals (lock with one, unlock with other)
- Cannot infer one from other easily
- How to encrypt? How to sign?

One way Functions



Mathematical Equivalents

- Factoring large numbers (product of 2 large primes)
- Discrete Logarithms

One-way Functions

- Computing $f(x) = y$ is easy.
- Eg. $y = 4^x \ mod\ 13$ (If x is 3, y is —?)

n	4^n mod 13	10^n mod 13
1	4	10
2	3	9
3	12	12
4	9	3
5	10	4
6	1	1
7	4	10
⋮	⋮	⋮

- Note: need not work with numbers bigger than 13 at all!
- But given y = 11, finding suitable x is not easy!
- Can do by brute-force (try all possibilities!)
- No method that is **much** better known yet!

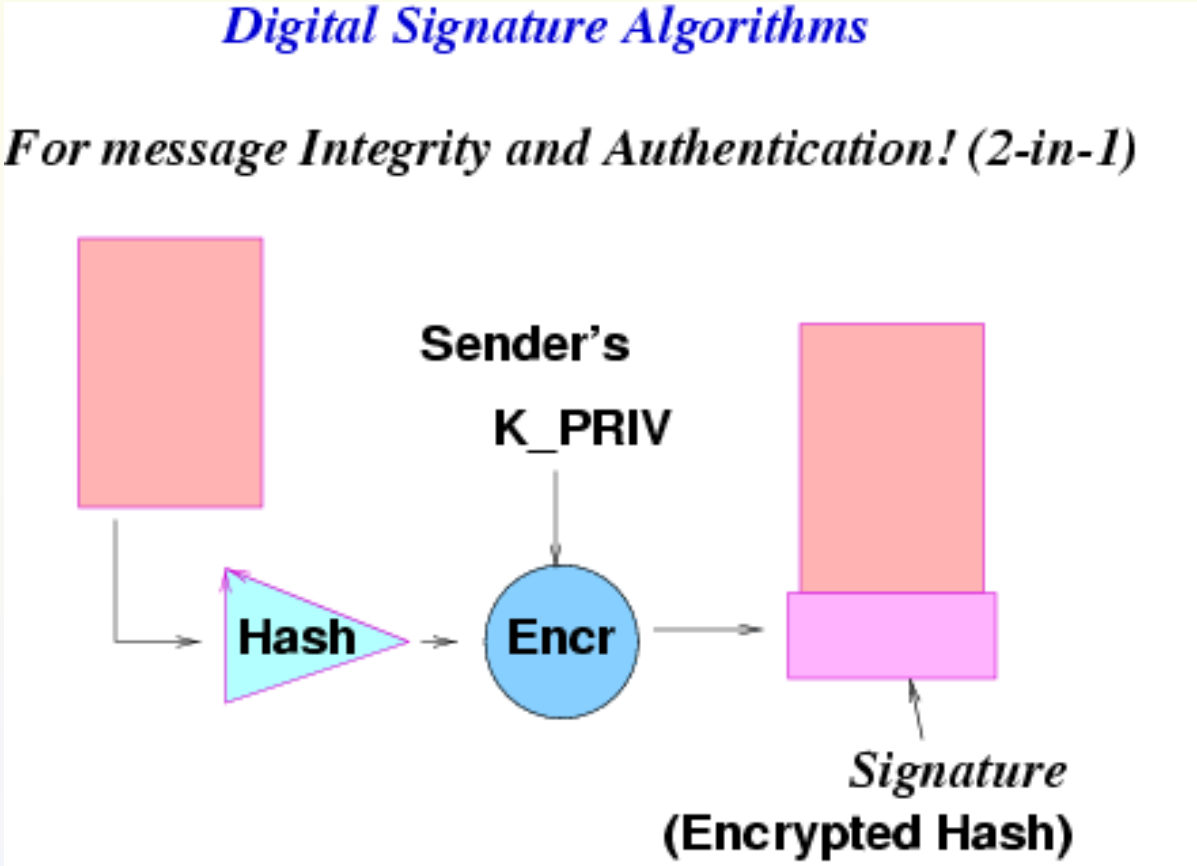
RSA Encryption Example

Pick 2 primes ($p = 251, q = 269$).
Let $n = p * q = 67519$ and $\phi(n) = (p-1) * (q-1) = 67000$.
Pick $e = 50253$ (relatively prime to $\phi(n)$).
Compute $d = e^{-1}\ mod\ \phi(n) = 27917$ (only one such d exists, with $(e * d)\ mod\ \phi(n) = 1$.
Interesting number-theoretic property for any $m < n$ is the following

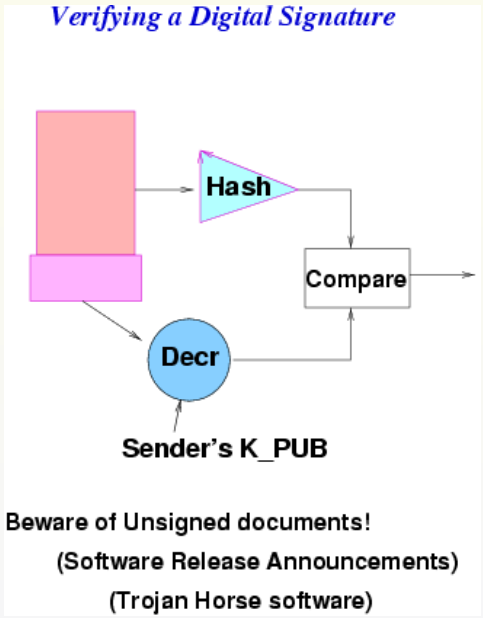
$$((m^e)\ mod\ n)^d\ mod\ n = m = ((m^d)\ mod\ n)^e\ mod\ n$$

Therefore to **encrypt** a message m take it 2 chars at a time (16 bits, so less than 65536) and compute $E(m) = m^e\ mod\ n$.
This is the **public** key (the numbers e, n).
Decrypting is done by $m = D(E(m)) = E(m)^d\ mod\ n$ and is easy only if d (**private key**) is known.

Digital Signatures

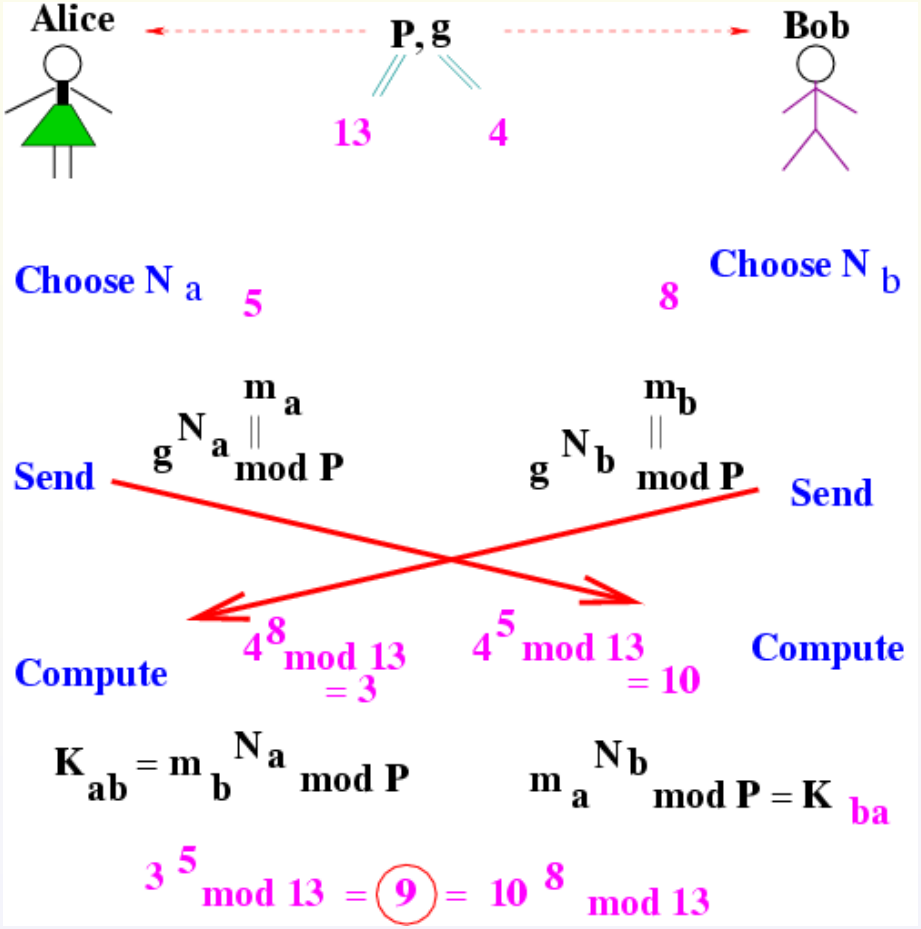


Verifying Signatures

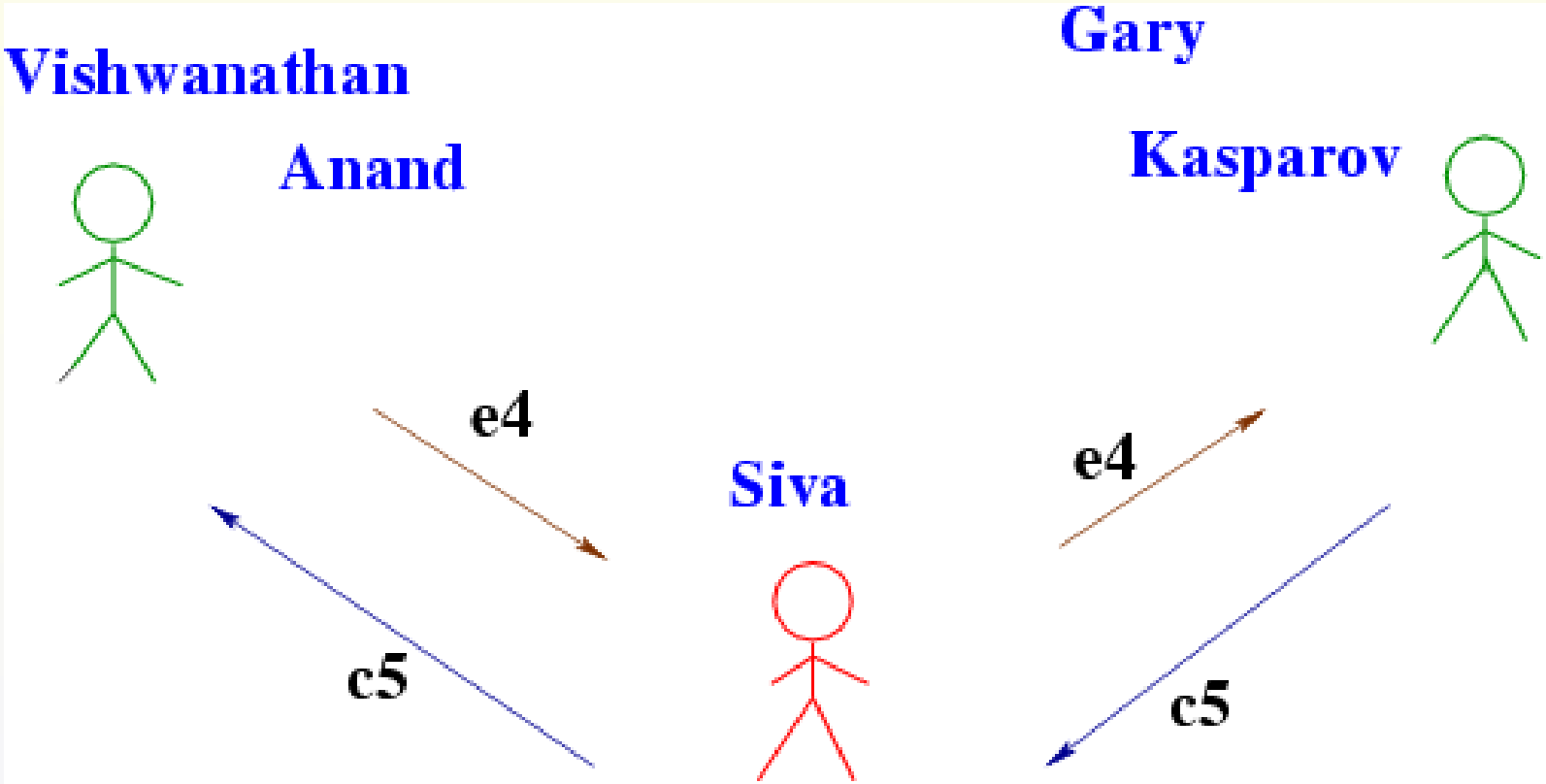


Digital Signatures provide three important security services
Integrity, Source Non-Repudiation, Authentication

Diffie-Hellman Key Establishment Protocol

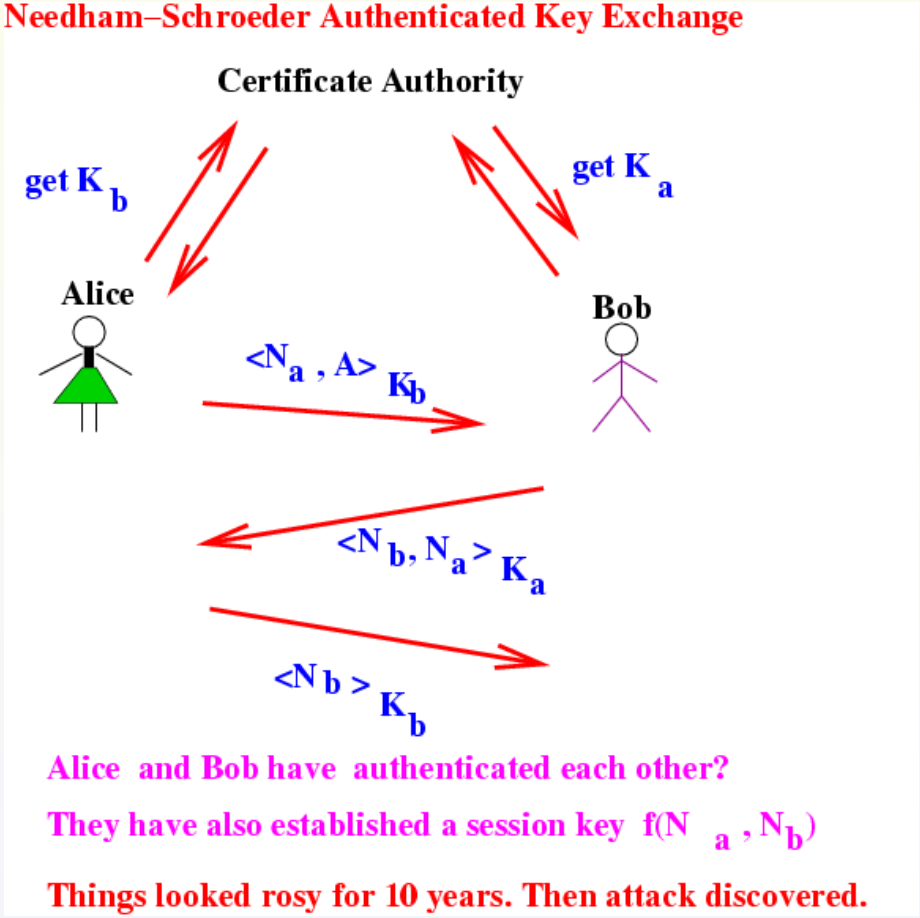


Man-in-the-middle attack

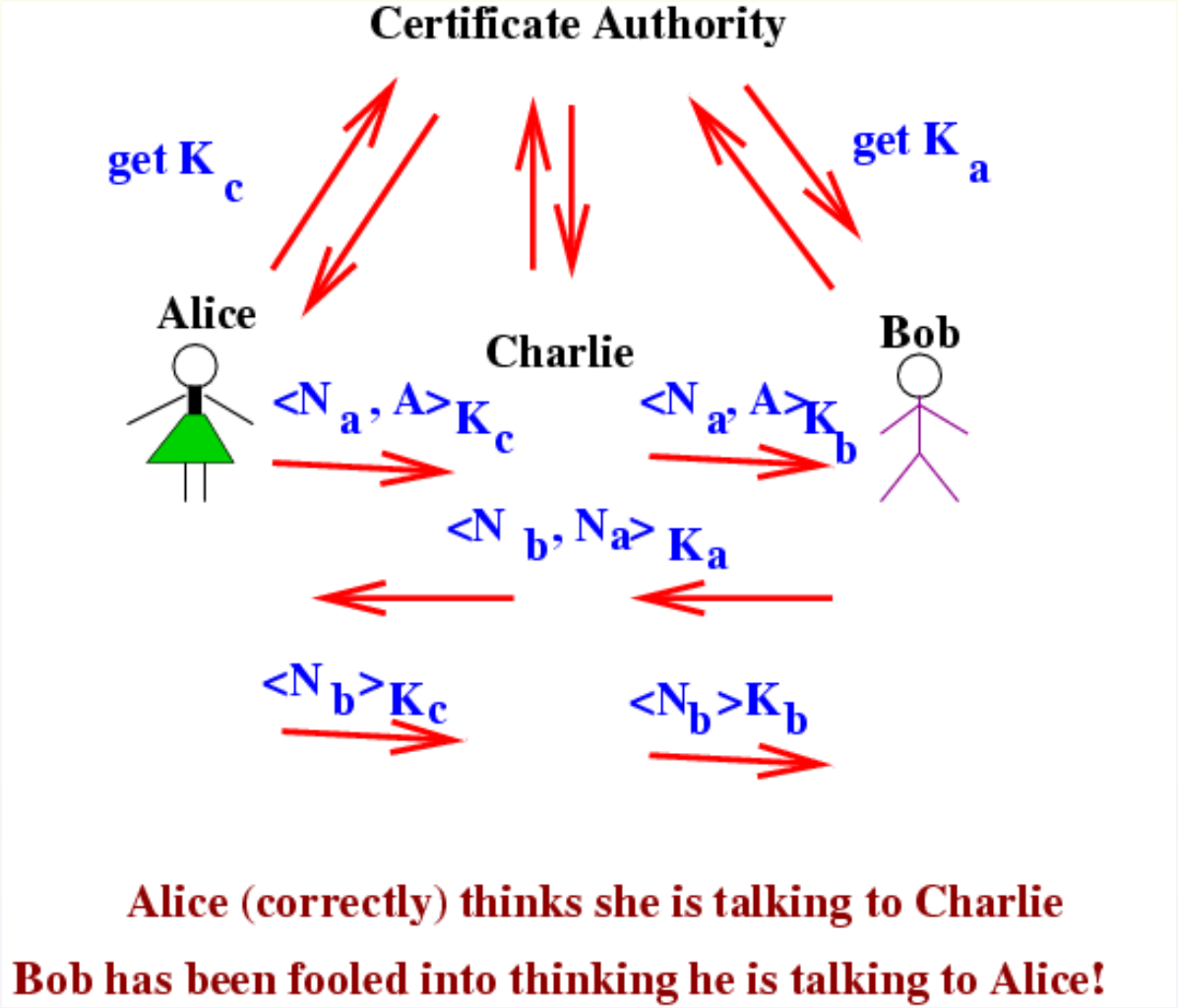


- Authentication was missing!
- Can be solved if Kasparov and Anand know each other's public key (Needham-Schroeder).

Needham-Schroeder Protocol



Attack by Lowe (1995)



Why Are Security Protocols Often Wrong?

They are *trivial* programs built from simple primitives, BUT, they are complicated by

- concurrency
- a hostile environment
  - a bad user controls the network
  - Concern: active attacks masquerading, replay, man-in-middle, etc.
- vague specifications
  - we have to guess what is wanted
- Ill-defined concepts

Protocol flaws rather than cryptosystem weaknesses
Formal Methods needed!

Online Voting Protocols

Are we ready for elections via Internet?

- George Bush (Nov 2000, dimpled chads)
- Pervez Musharaf (April 2002)
- Maharashtra (Oct 13, 2004)

E-Voting Protocols Requirements

- No loss of votes already cast (reliability)
- No forging of votes (authentication)
- No modification of votes cast (integrity)
- No multiple voting
- No vote secrecy violation (privacy)
- No vulnerability to vote coercion
- No vulnerability to vote selling or trading protocols (voter is an adversary)

Other Desirable Properties

Must not only be correct and secure, but also be seen to be so by skeptical (but educated and honest) outsiders.

- Auditability:
  Failure or procedural error can be detected and corrected, especially the loss of votes.
- Verifiability: Should be able to prove
  - My vote was counted
  - All boothes were counted
  - The number of votes in each booth is the same as the number of people who voted
  - No one I know who is ineligible to vote did so
  - No one voted twice
  - ...

without violating anonymity, privacy etc.

Zero Knowledge Proofs

References

- Books
  - *TCP/IP Illustrated* by Richard Stevens, Vols 1-3, Addison-Wesley.
  - *Applied Cryptography - Protocols, Algorithms, and Source Code in C* by Bruce Schneier, Jon Wiley & Sons, Inc. 1996
  - *Cryptography and Network Security: Principles and Practice* by William Stallings (2nd Edition), Prentice Hall Press; 1998.
  - *Practical Unix and Internet Security,* Simson Garfinkel and Gene Spafford, O'Reilly and Associates, ISBN 1-56592-148-8.
- Web sites
  - *www.cerias.purdue.edu* (Centre for Education and Research in Information Assurance and Security)
  - *www.sans.org* (System Administration, Audit, Network Security)
  - *cve.mitre.org* (Common Vulnerabilities and Exposures)