Big Numbers:

The Role Played by Mathematics in Internet Commerce

Dr. David Singer (Dept. of Mathematics, CWRU)
and
Mr. Ari Singer (NTRU Cryptosystems)

Public Key Cryptography

Alice and Bob have never met before. Yet they are able to carry on a private conversation on an insecure communications channel

and not worry about eavesdroppers.

How is this possible?

Carol and David are flipping a coin

over the telephone, and each is confident the other is not cheating.

How is this possible?

Ethel has a secret.

She wants to convince Fred that she knows the secret, but without revealing anything about the secret to him.

How is this possible?

Cryptography

- Cryptography (secret writing), is the art and science of secure transmission of confidential information.
- It also allows secure storage of data.
- Only someone with the *key* can get access.

"Classical" Cryptography

- Dates back to antiquity
- Alice and Bob agree on a method of *encryption* and a shared secret *key*.
- Alice uses the key to encrypt the message she sends.
- Bob uses the same key to *decrypt* the message.

Classical Cryptanalysis

- Oscar attempts to determine the contents of an encrypted message without the key.

He may try all possible keys (Brute force)

Or he may use more subtle techniques, such as analysis of statistical anomalies.

Modern Cryptography

New Directions in Cryptography,

by Whitfield Diffie and Martin Hellman, 1976.

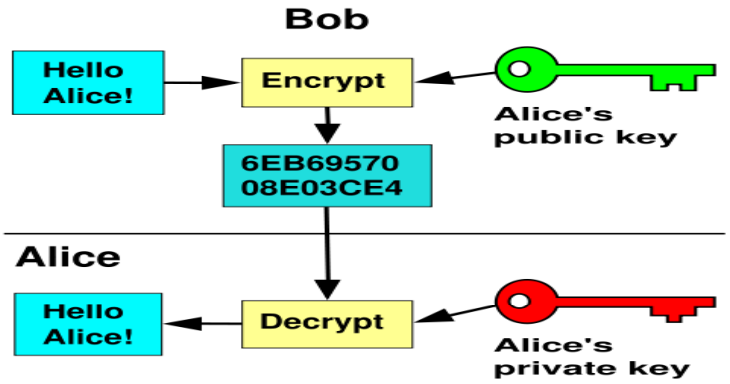
(Also classified publication by James Ellis in 1970, declassified in 1997.)

Introduced the essential idea:

Public Keys and Private Keys.

Bob has two keys: a public key, which is available to anyone, and a private key.

Alice uses the public key to lock (encrypt); Bob uses the private key to unlock (decrypt).

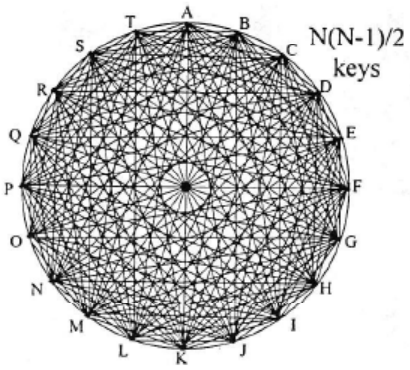


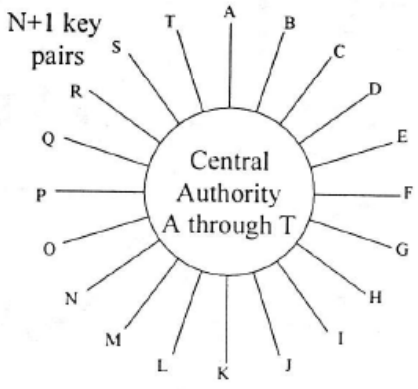
Advantages

- Alice can communicate without having previously contacted Bob.
- No one but Bob can decrypt the message.
- Major reduction in the number of keys required for a large group.

Public key v.s. Private key

- Private key: 20 users need 190 key pairs
- Public key: 20 users need 21 key pairs





Disadvantages

- Public-Key Cryptography tends to be slower
- May be harder to implement in a secure way

Big question: How can it be made To work??

Mathematics

Creating a mathematical secret

- It is easy to multiply numbers.
- There are usually many ways to get the same product:

$$18 \times 2 = 12 \times 3 = 9 \times 4 = 6 \times 6 = 36$$

But if two *primes* are multiplied together there is only one way to 'unmultiply' (factor) them

$$7 \times 5 = 35$$

Creating a mathematical secret

- Multiplying numbers is "easy"
- But factoring numbers is "hard"

$$10818814513071979293 83 =$$

$$4706321191 \; ? \times ? \; 2987837153$$

Basis for RSA cryptosystem:
L.M. Adleman, R.L. Rivest and A. Shamir, 1978

The RSA Cryptosystem

- Generate two large prime numbers p and q. Multiply them together to get very large number N.
- Compute Euler Totient T=(p-1)(q-1)
- Choose numbers e and d for which the product e times d leaves remainder 1 when divided by T.
- Publish (N, e) (this is the public key).
- Keep the rest secret.

The Encryption algorithm

- Turn message into a large number m (*encoding*)
- Compute $c = m^e \mod N$ (this is the remainder left when m^e is divided by N).
- The number c is the encryption of the message!

(Don't Panic!)

The Decryption Algorithm

- Compute $m = c^d \mod N$
- Decode m to get the message.
- Mathematical principle: If you know the values of m, e, and N, you can compute c.
- If you know the values of c, d, and N, you can compute m.
- BUT if you know c, e, and N and can't factor N, you (probably) can't get m.

A Small Example: N=33

$$N = 33, e = 3, d = 7$$

$$m = 8$$

$$m^3 = 512 = 33 \times 15 + 17$$

$$c = 17$$

$$c^7 = 410338673 = 33 \times 12434505 + 8$$

$$m = 8$$

Big Primes

The largest known prime is a *Mersenne* Prime, a number of the form

$$2^p - 1$$

where p is a prime number. Only 42 such numbers have been found so far. The largest one, found in September 2006 , is

$$2^{32582657} - 1$$

Big Primes

It has 9,808,358 digits; if you want to see them, visit

http://www.mersenne.org/prime.htm

These large primes do not currently have any practical application in cryptography.

Factoring into Big Primes

RSA-200 was factored the team of F. Bahr, M. Boehm, J. Franke, and T. Kleinjung.

At 663 bits, RSA-200 is the largest RSA Challenge Number factored to date. (There are no more challenge problems.)

The sieving effort is estimated to have taken the equivalent of 55 years on a single 2.2 GHz Opteron CPU. The matrix step reportedly took about 3 months on a cluster of 80 2.2 GHz Opterons. The sieving began in late 2003 and the matrix step was completed in May 2005.

Factoring into Big Numbers

RSA 200 =
27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

= 35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883491

×

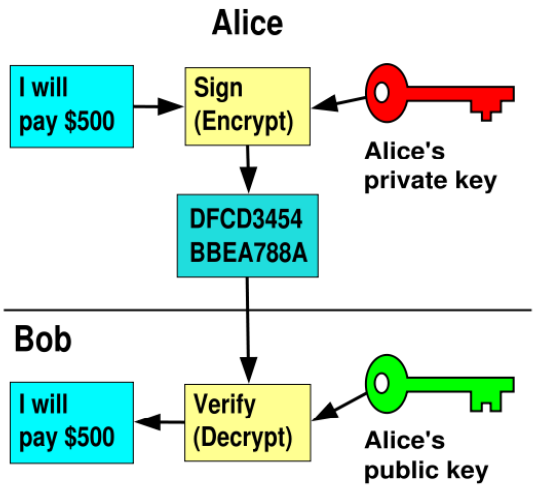
79258699544783330333470858148005968773797585736421996073433034145576787281815213538140930474018546 7

Digital Signatures

RSA can also be used to allow Alice to sign a document. She *decrypts* the document with her secret key. Anyone else can use her public key to see that she signed it.

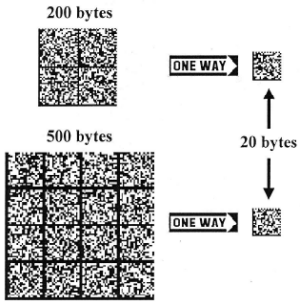
Digital Signatures

- Only Alice can use her key to sign a message:

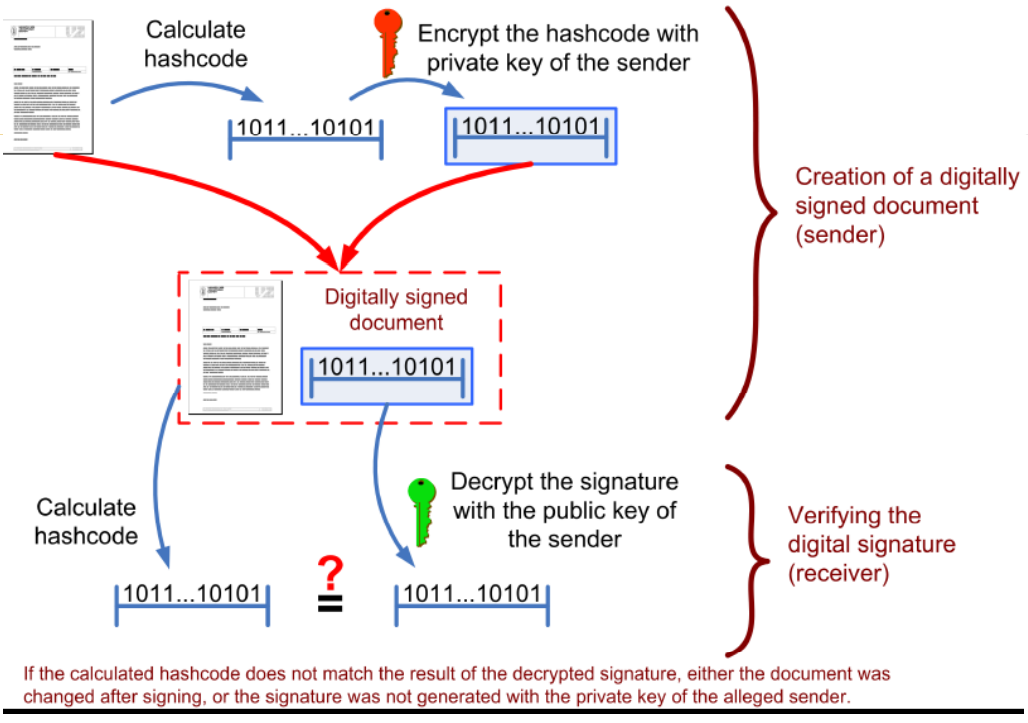


Secure Hash Function

- In practice, Alice does not sign the message itself; she signs a hash (a compressed version).
- This makes electronic forgery much more difficult.



Creating and verifying a digital signature



Mathematical tools

- Number theory –for encryption algorithms.
- Computational complexity – to know what is hard and what is easy to compute.
- Probability theory – randomness is needed for implementing algorithms securely.

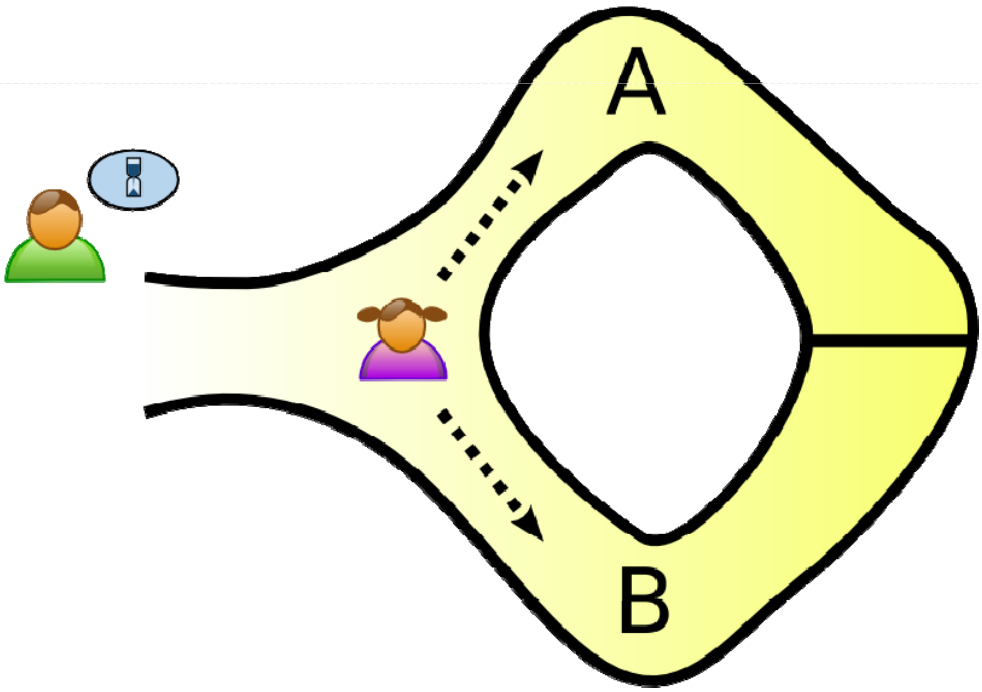
Mathematical Tools

- Computational Mathematics – to know how to make calculations quickly and accurately.
- Other mathematics: linear algebra, geometry,…

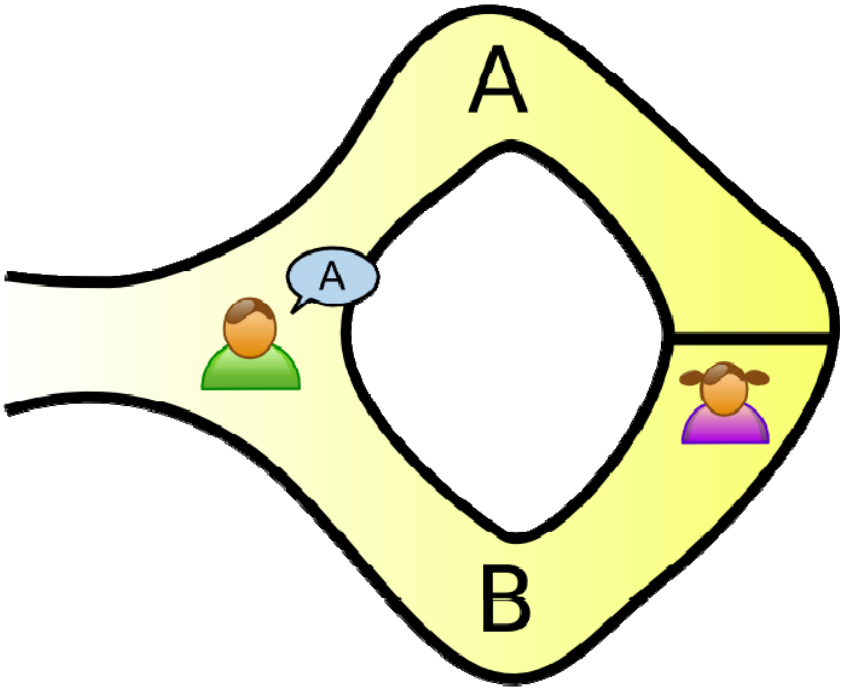
Challenge-response

- To prove identity, you possess a secret (password).
- But you don't want to give up the secret! (Remember Ethel and Fred)
- So you must give a "proof of knowledge."

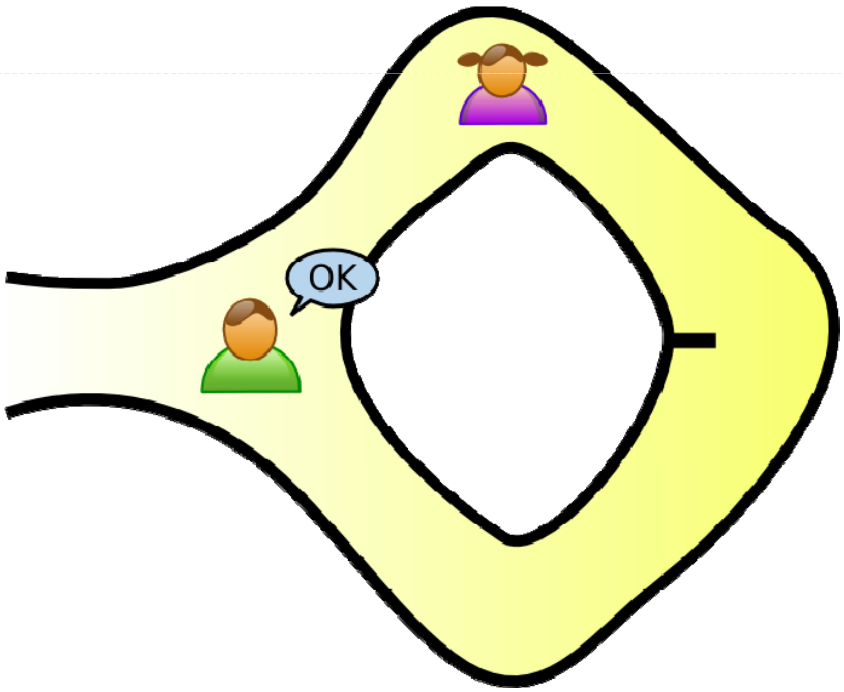
Ali Baba's Cave



Ali Baba's Cave



Ali Baba's Cave



Zero-Knowledge Proof

- Using challenge-response techniques, Alice demonstrates she knows the password (with high probability) but does not reveal the password.
- She may have to respond to many challenges in order to convince Bob.
- Key idea for solving many problems

(e.g., coin-flip over telephone)

Why Use Cryptography?

- We are protecting data and there is a lot of data to protect!

What are we protecting against?

- Well known stuff like
  - Laptop loss or theft
  - Data center compromise
  - Viruses
  - Hackers
  - Snooping of e-mail and personal data
- And lesser known stuff like
  - Electronically modifying sensor data in a factory
  - My neighbor changing the temperature on my refrigerator

Cryptographic Services

- Privacy (encryption) – You can't see it
- Integrity (signing) – You can't change it
- Authentication (validation) – I wrote it
- Freshness (challenge-response) – I am doing this now

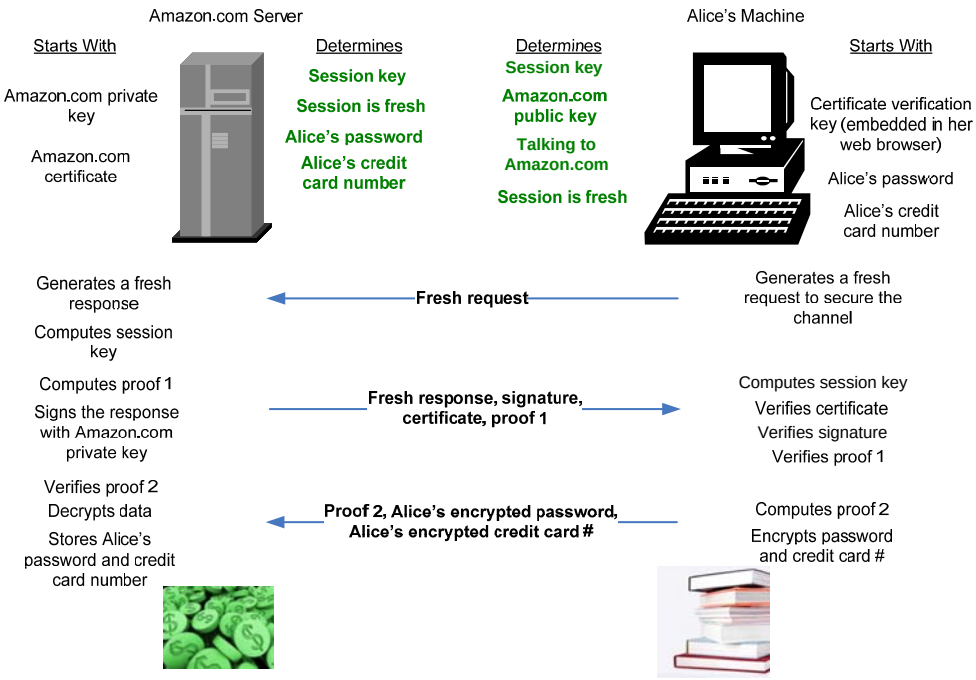
Common Security Goals

- Protection of data (access control)
  - Secrecy of data (read access)
  - Creation of data (write access)
- Authentication required to access resources
  - Networks, individual machines, etc.
- Proof of authorization of an action
  - Signature on a contract, authorization of payment, etc.

Security Goals: Authentication

- Web sites – Am I at Amazon.com?
- Users– Is this Alice trying to access the site?
- Network devices – Is this the DNS server that really knows which machines host amazon.com?

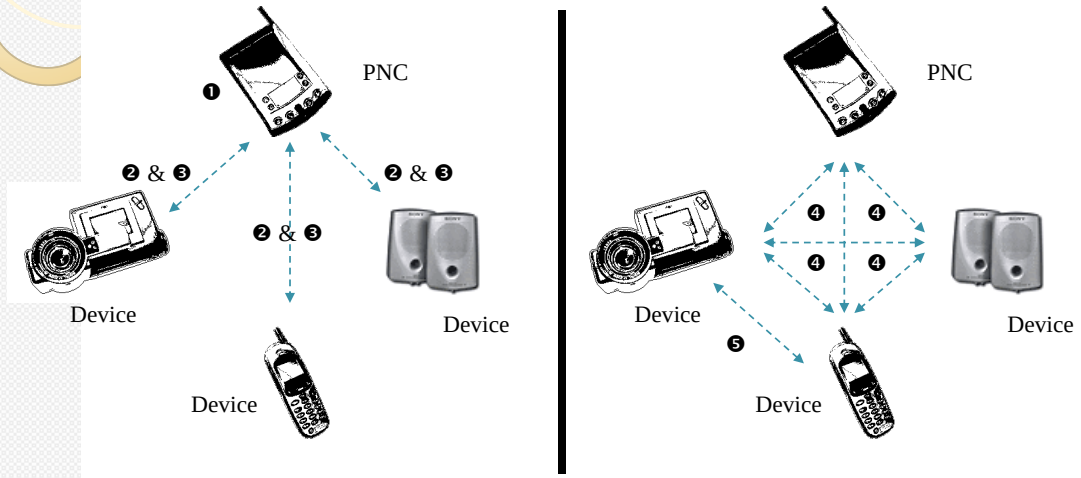
Example: Web Authentication



Security Goals: Data Secrecy

- Data at rest
  - Databases (e.g. with credit card numbers), hard drive contents, tape drive contents
- Data in transit
  - Premium cable content, phone conversations, e-mails, internet traffic, industrial sensors

Example: Wireless Personal Area Network (WPAN)



❶Devices determine which device is best suited to be piconet controller (PNC) and agree on it.

❷Each device requests to join the piconet and performs mutual authentication with the controller.

❸The controller establishes time slots for each device and distributes piconet payload protection keys.

❹Devices transmit protected data to the other devices in the piconet during their time slots.

❺Two devices may optionally establish their own secure sub-network.

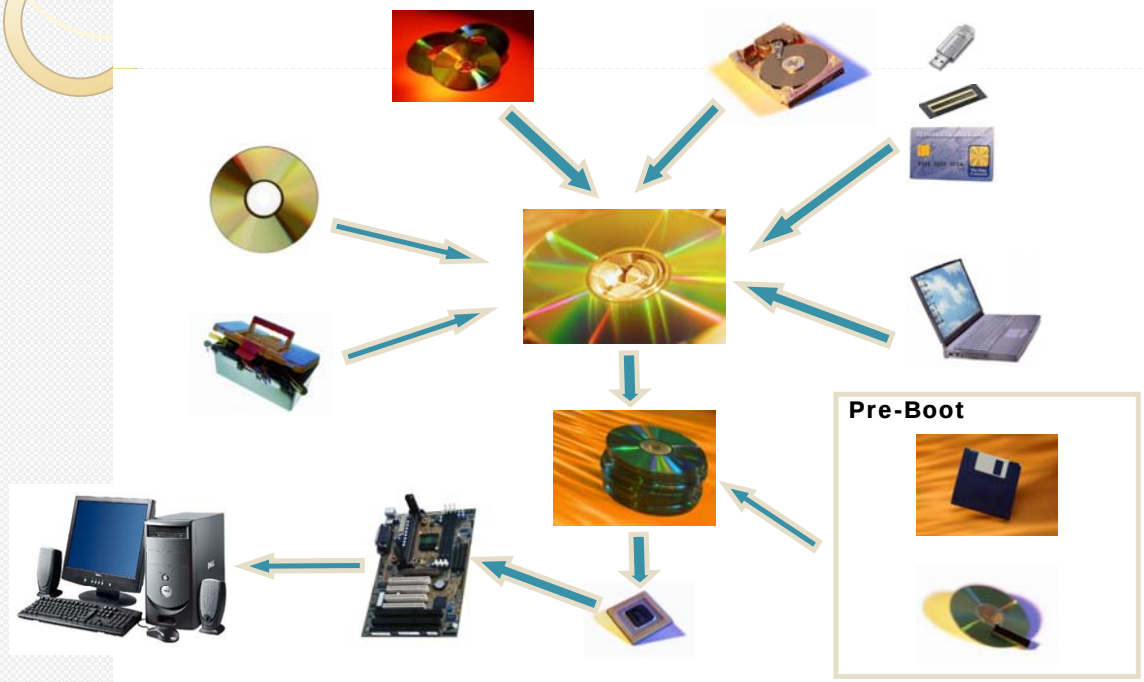
Building the Solution

- Complexity of requirements on data management often translates to complexity of security models
- Many companies must come together to create new and better security solutions to meet these new needs
- Solutions must balance three competing forces:
  - Cost
  - Ease of use
  - Security

Example: Trusted Computing

- Goal is to ensure that the hardware and software on your machine is behaving properly
- Inclusion of a Trusted Platform Module (TPM) on a platform assists in building trust in your machine
- Many pieces must come together to make this work in practice

Example: Trusted Computing Ecosystem



Do You Use Cryptography?

- Do you buy anything online?
- Do you pay your bills or bank online?
- Do you use SpeedPass?
- Do you watch cable TV?
- Do you ever pay for Internet access when away from home?
- Do you access your employer's network from outside of your office?
- Do you like to buy the latest gadgets?