Introduction to Computer Security

Carmela Troncoso, KU Leuven (COSIC)

Computer Security Course, University of Vigo

20th-July-2009

Acknowledgements: Prof. Vincent Rijmen and Prof. Bart Preneel

Remark 1

What this course ***is*** about

“Technical” side of Computer Security

What this course ***is not*** about

Regulations and legal compliance

Remark 2

You are my Guinea Pigs

(suena mejor en español: conejillos de indias)

Apologies in advance!

Course outline

- Introduction (1h)
  - Motivation
  - Security properties
  - Main building block: cryptography
- Authentication (1h)
  - Passwords
  - Challenge-response protocols
  - Biometrics

Course Outline

- Computer Security (2h)
  - Key concepts
  - Access List Control vs Capabilities
  - Security models
  - Certification

- Network Security (2h)
  - Protocols
  - Internet threats
  - Defenses
  - Peer-to-peer

Course Outline

- Embedded Security (2h) (by Benedikt Gierlichs)
  - Motivation
  - Issues
  - Physical security

- Privacy Enhancing Technologies (2h)
  - Motivation
  - Anonymous authentication
  - Anonymous communications
  - Measuring privacy
  - Location Privacy

Not-covered security topics

- Database security
- Software security
- Cryptography and cryptanalysis
- Wireless security
- Usability, HCI
- e-Voting
- Steganography
- Watermarking
- Legal aspects
- ...

Outline for today

- Motivation
- Let’s get a bit formal
- DOs and DON’Ts
- Cryptography as a building block
- Conclusions

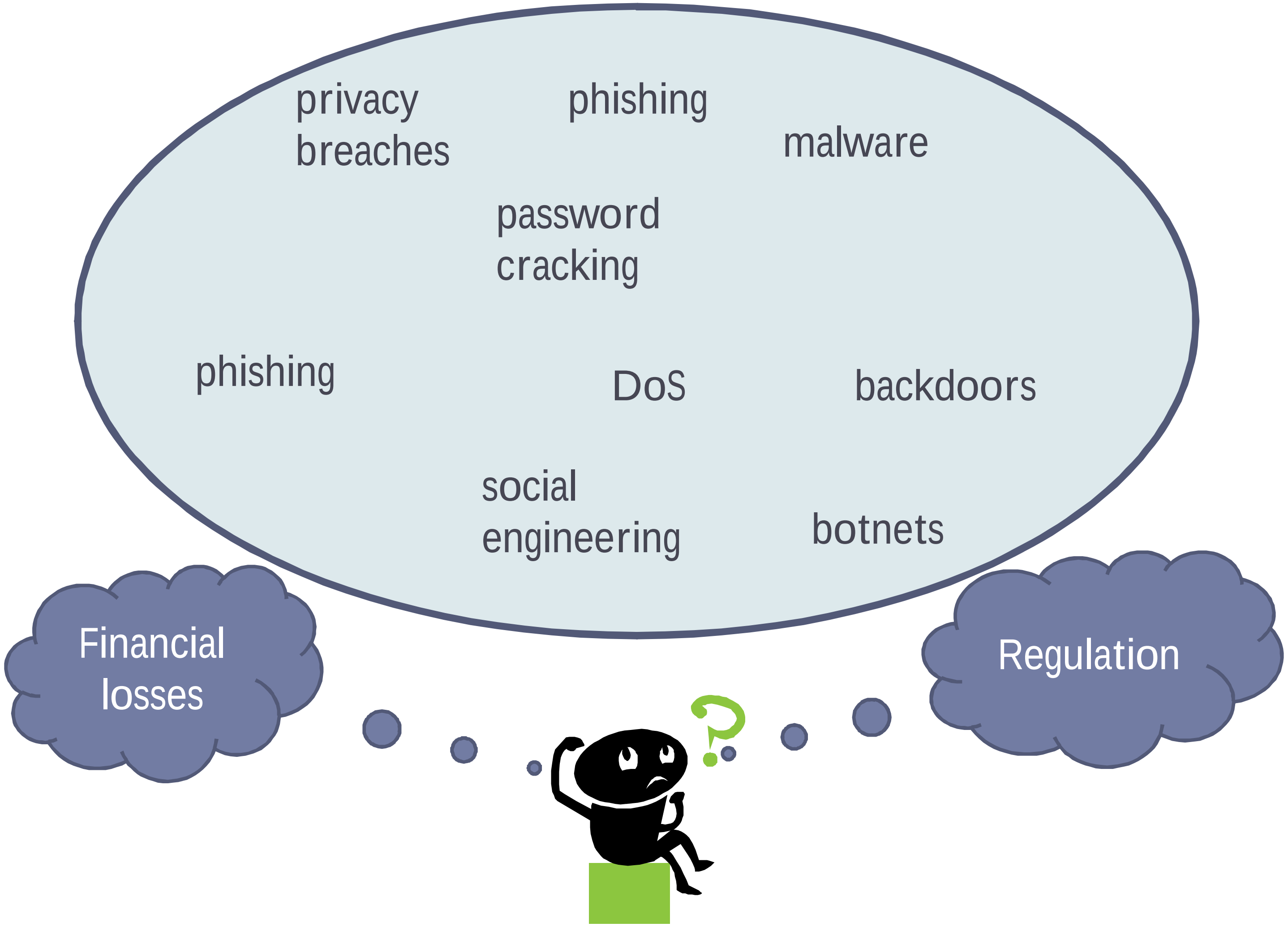
Fear, Uncertainty and Doubt

- Main driving reasons
  - Need to protect valuable assets
  - *“my product is better than yours...”*

- e-security as ‘e-nabler’
  - is actually the most efficient

- Technology is **not** enough
  - Security needs also procedures
  - (although I will mostly speak about the technical side)

The need for e-security



privacy breaches

phishing

malware

password cracking

phishing

DoS

backdoors

social engineering

botnets

Financial losses

Regulation

Business perspective

- Direct Losses
  - Theft
    - Money
    - Confidential Information
    - IT material
  - Productivity loss
    - Reconfiguration
    - Recovery (not only data)

- Indirect Losses
  - Secondary loss
    - Company image
    - Competitive advantage
    - Sales
  - Legal exposure
    - Privacy regulations
    - Contract breach
    - Legal obligations

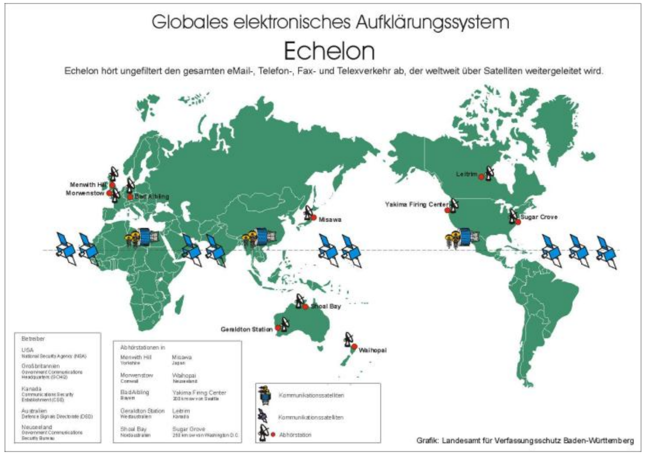
- Many fields: e-banking, e-commerce, e-business, e-government, e-id,...

Echelon

- Signals Intelligence Collection Network (UKUSA)
  - UK,
  - USA,
  - Australia,
  - Canada,
  - New Zealand

- Inspection of telephone calls, fax, e-mail and other data traffic

- Reportedly militar
  - Allegedly
    - Other national security issues
    - industrial espionage



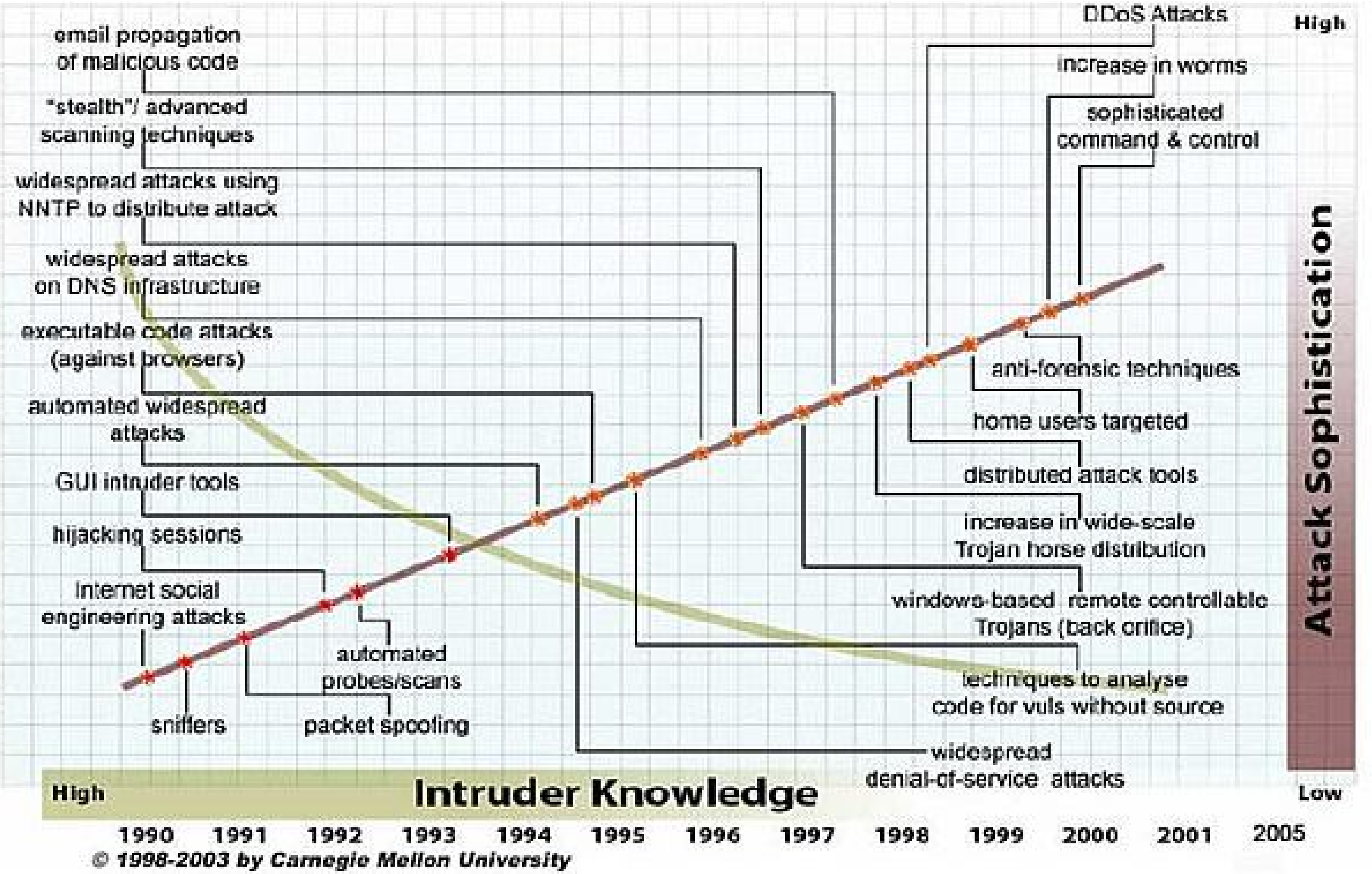
Source: Landesamt fur Verfassungsschutz Baden-Wurttemberg

Who attacks IT systems?

- Nation-states
  - Echelon
- Organized crime
  - botnets, spam, espionage
- Skilled hacker
  - money, ideology, intelectual challenge
- Unskilled hacker (“script-kiddie”)
  - revenge, just-for-fun

- Threats
  - Disclosure: Snooping, sniffing
  - Deception: Modification, spoofing, repudiation of origin, denial of receipt
  - Disruption: Modification , delay, denial of service
  - Usurpation: privileges raise, session hijacking

Security trends

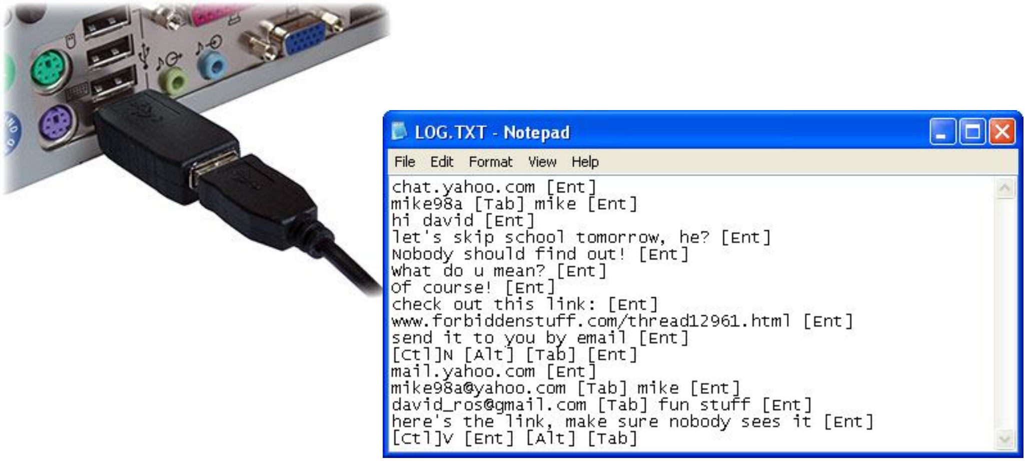


An example: keystroke logger

- Plug and play

Key Katcher
256Kb - $60

Source: http://www.thinkgeek.com/



```
chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
what do u mean? [Ent]
of course! [Ent]
check out this link: [Ent]
www.forbiddenstuff.com/thread12961.html [Ent]
send it to you by email [Ent]
[Ctl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
here's the link, make sure nobody sees it [Ent]
[Ctl]v [Ent] [Alt] [Tab]
```

KL2 Keylogger
2Mb - $150

Source: http://www.diij.com/

- Huge memory capacity organized as a flash file system
- Compatible with all USB keyboards (including Linux & Mac)
- Transparent to computer operation, undetectable for security scanners
- No software or drivers required, operating system independent
- Quick and easy national keyboard layout support
- Ultra compact and discrete, only 2" long (extends just 1.5" when plugged in)

or Aircrack

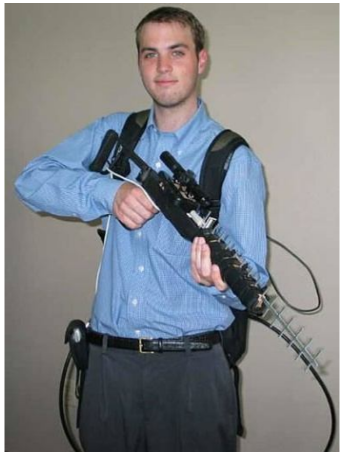
> *“Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It* ***implements the standard FMS attack*** *along with some* ***optimizations like KoreK*** *attacks, as well as* ***the all-new PTW attack****, thus making the attack much faster compared to other WEP cracking tools.”*

http://www.aircrack-ng.org/

- KoreK attacks based on *Weaknesses in the Key Scheduling Algorithm of RC4,* S. Fluhrer, I. Mantin, A. Shamir in Selected Areas of Cryptography (2001)
  - RC4 designed by Ron Rivest (RSA Security) in 1987
- Freeware, only need a few clicks

and not only your neighbour should be worried

- **Tom’s guide: How To Build a BlueSniper Rifle**
  - <400€
  - Bluetooth
  - 1km

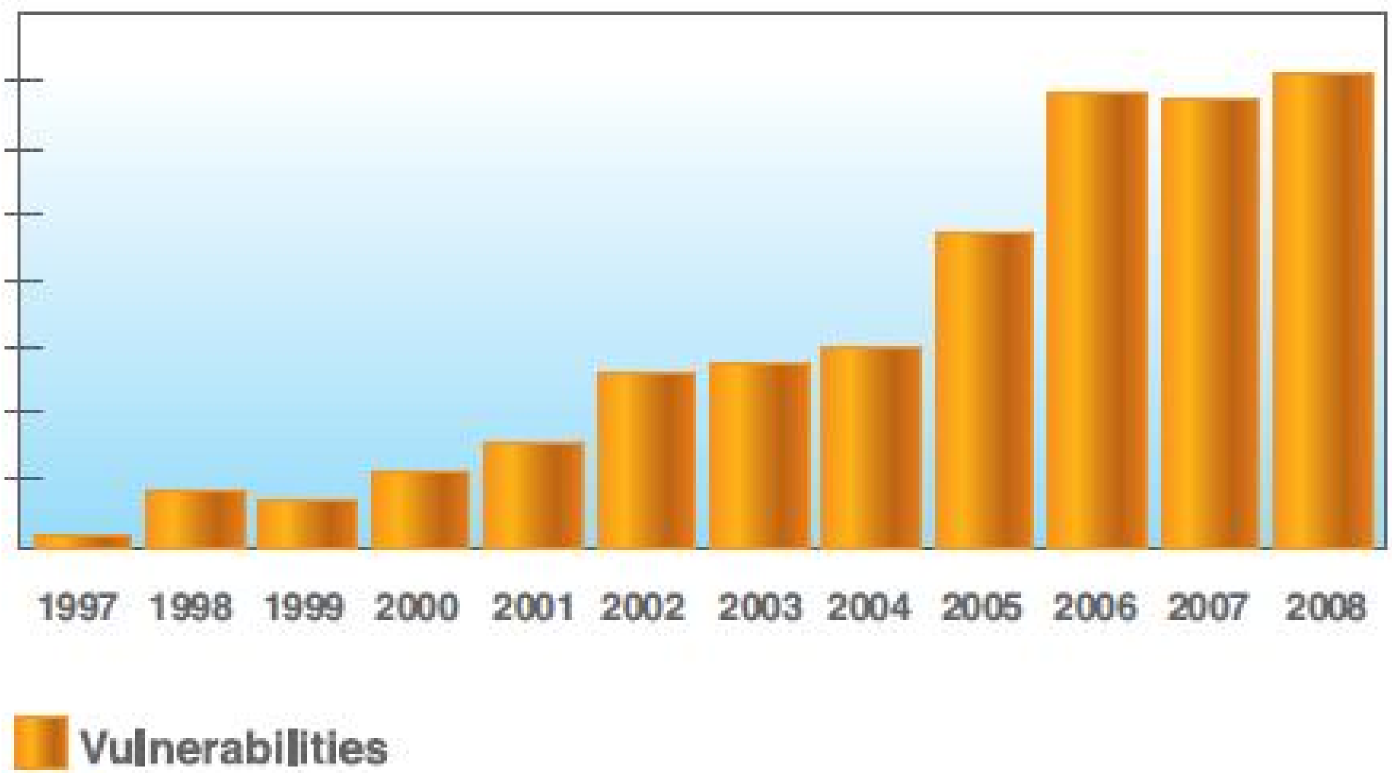


Source: http://www.tomsguide.com

- Pringles Cantenna:
  - <10$ and ~1h
  - WiFi
  - http://www.oreillynet.com/cs/weblog/view/wlg/448

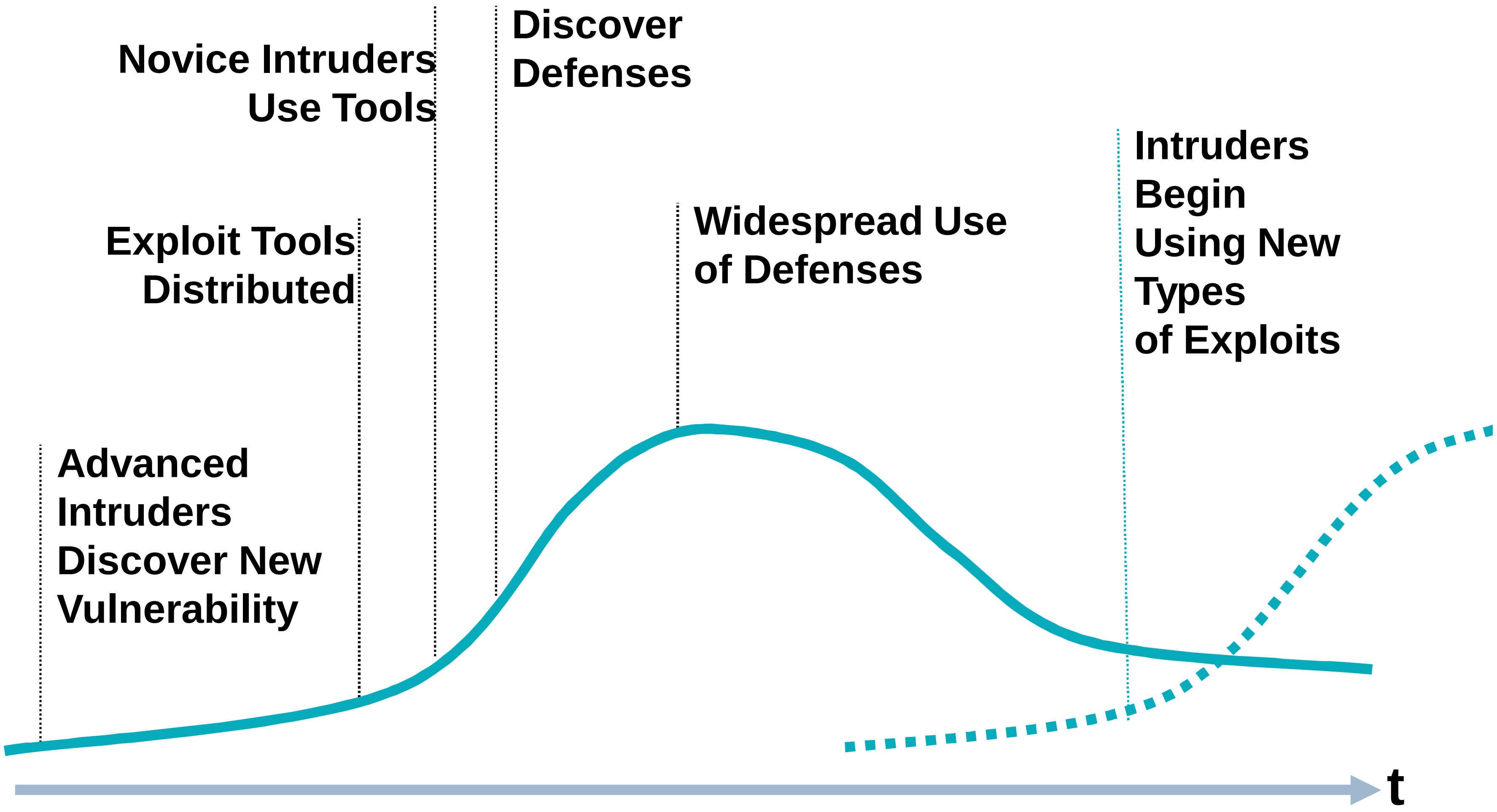
which results in...

- Vulnerability: spam, phishing, browser exploitation, malware



Source: IBM Internet Security Systems X-Force® 2008 Mid-YearTrend Statistics

Window of exposure



Source: CERT Centers, Software Engineering Institute (Carnegie Mellon University)

Process approach to security

- Security deals with the protection of valuable assets
  - Car, home, family, oneself, thoughts

- e.g., securing your home

1. *Prevention*: avoid damage
   - House locks, widow bars, burglar alarm
2. *Detection*: detect what happened and who did it
   - Alarm goes off, objects disappear
3. *Reaction*: recovery
   - Police recovers object, replace object, ...

...and Computer security?

- Increasingly moving to electronic assets (records, transactions, shopping,...) is it the same situation?

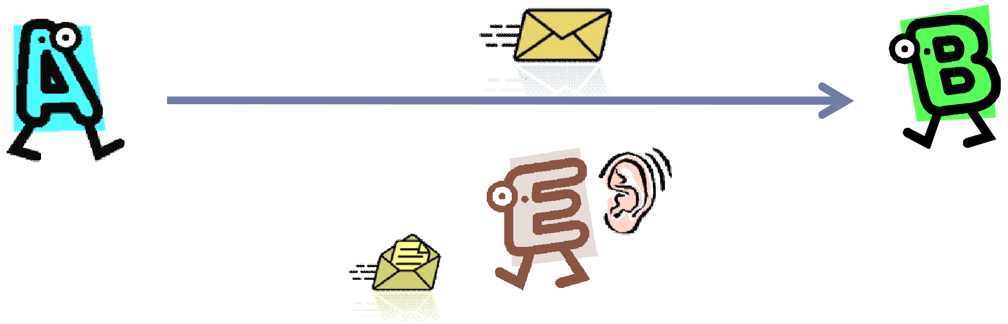
- e.g., card fraud on internet transaction
  - *Prevention*: avoid damage
    - Encryption
  - *Detection*: detect what happened and who did it
    - Bank statement
  - *Reaction*: recovery
    - Ask for new number, reimboursment of transaction

- Not exactly the same

Security properties

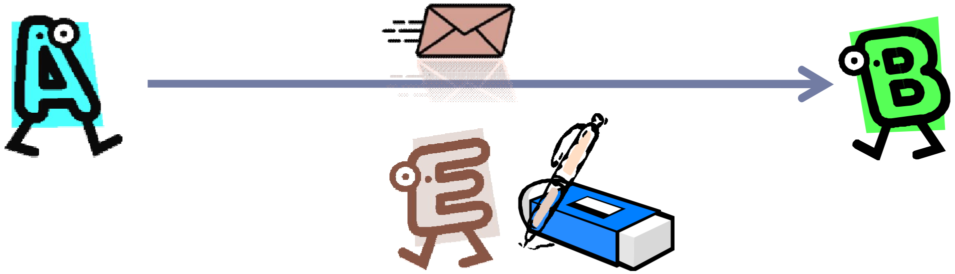
- Traditionally: **CIA**
  - Confidentiality
  - Integrity
  - Availability

- **Confidentiality**
  - prevention of unauthorized disclosure of information



Security properties (II)

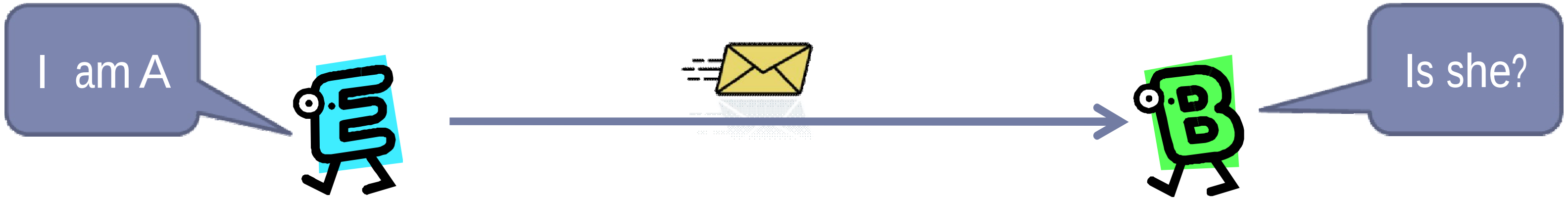
- **Integrity**
  - prevention of unauthorized modification of information



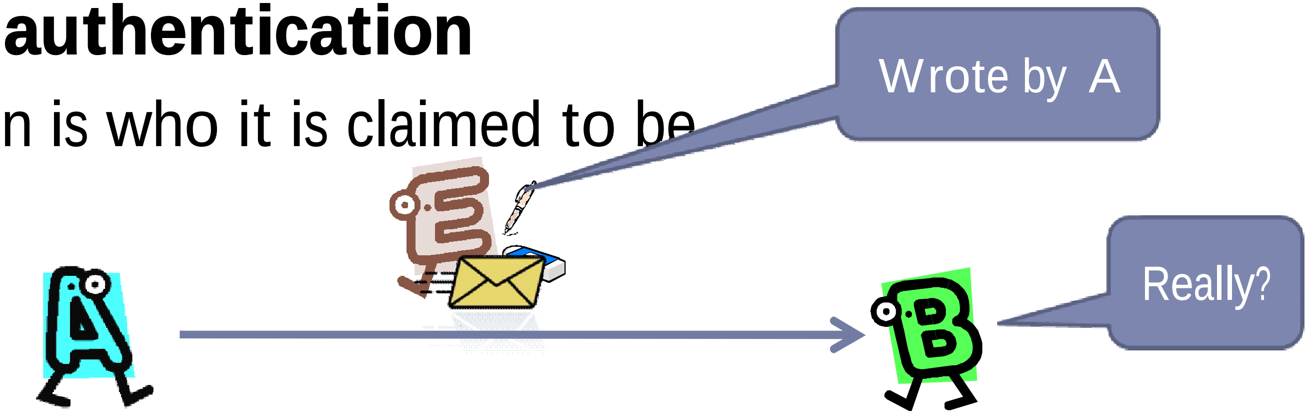
- **Availability**
  - prevention of unauthorized denial of service

Security properties (III)

- **Entity authentication**
  - sender is who he is claiming to be



- **Data authentication**
  - origin is who it is claimed to be



Security properties (IV)

- **No repudiation (origin)**
  - the sender cannot repudiate having sent a message

- **No repudiation (destination)**
  - the receiver cannot repudiate having received a message

I didn't receive

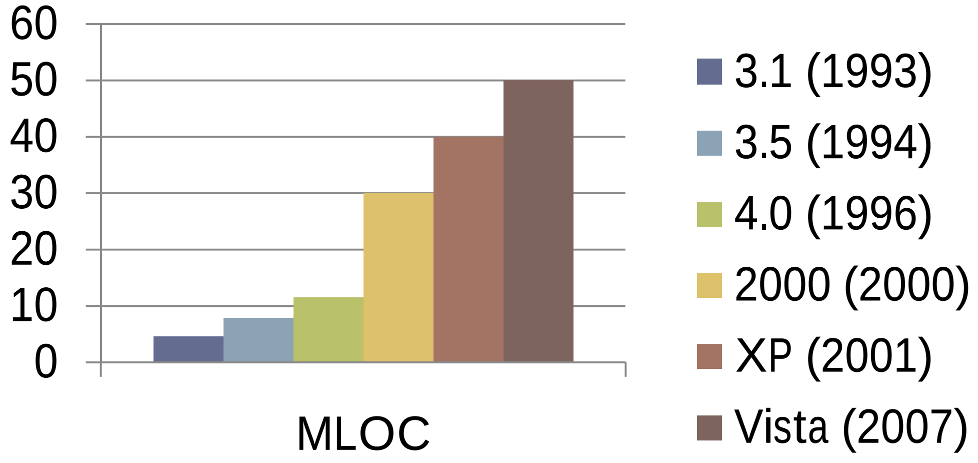
More

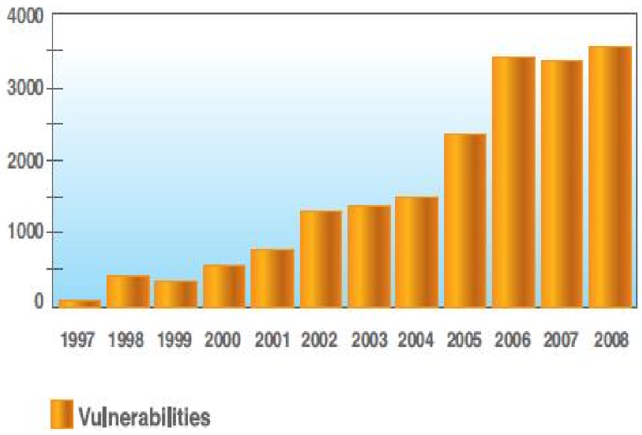
- **Auditability**
  - Should be possible to track back the offender
- **Privacy properties**
  - Anonymity (confidentiality of identity)
  - Unlinkability
  - Pseudonimity
  - Unobservability
- …

DOs and DON’Ts

Information security principles **DON'Ts**

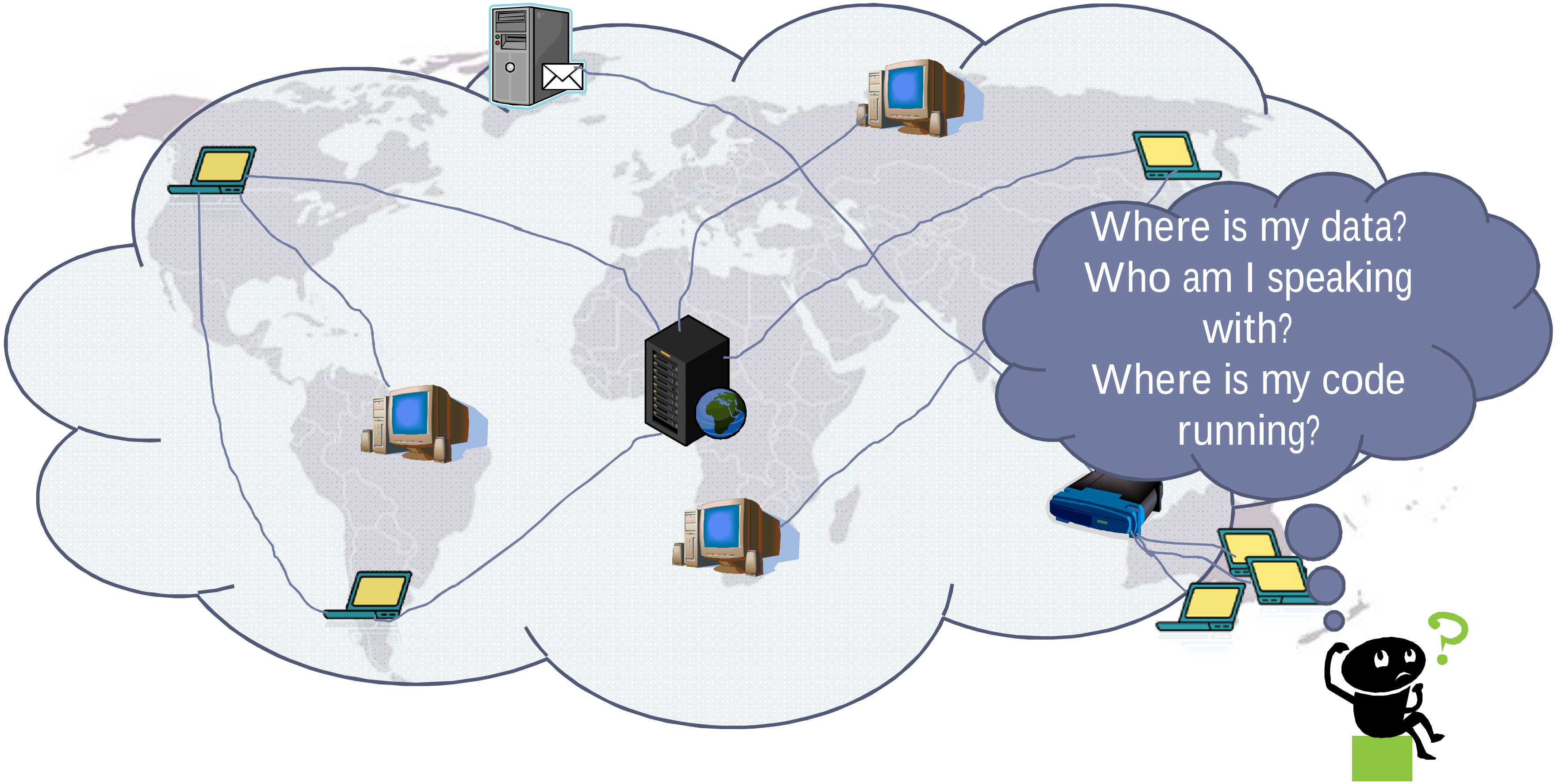
- Security and complexity **do not** mix
  - O/S
  - Applications
  - Mobile code
  - Services:VoIP, IM
  - Always connected...





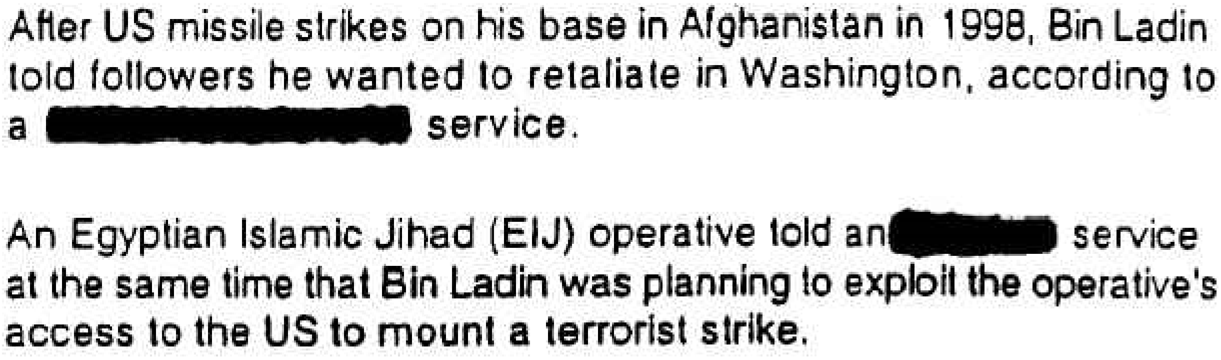
Information security principles **DON'Ts**

- Security and complexity **do not** mix: Internet is complex!



Information security principles **DON’Ts**

- Security by obscurity **does not** work
  - GSM encryption algorithm reverse engineered
  - DVD copyright protection by-passed
  - Cisco operating system
  - Microsoft products vulnerabilities
  - MIFARE cards
- David Naccache “decrypts” CIA declassified document



After US missile strikes on his base in Afghanistan in 1998, Bin Ladin told followers he wanted to retaliate in Washington, according to a [redacted] service.

An Egyptian Islamic Jihad (EIJ) operative told an [redacted] service at the same time that Bin Ladin was planning to exploit the operative's access to the US to mount a terrorist strike.

Source: http://www.globalsecurity.org/intell/library/reports/2004/pdb_6august2001-declass.pdf

Information security principles **DON’Ts**

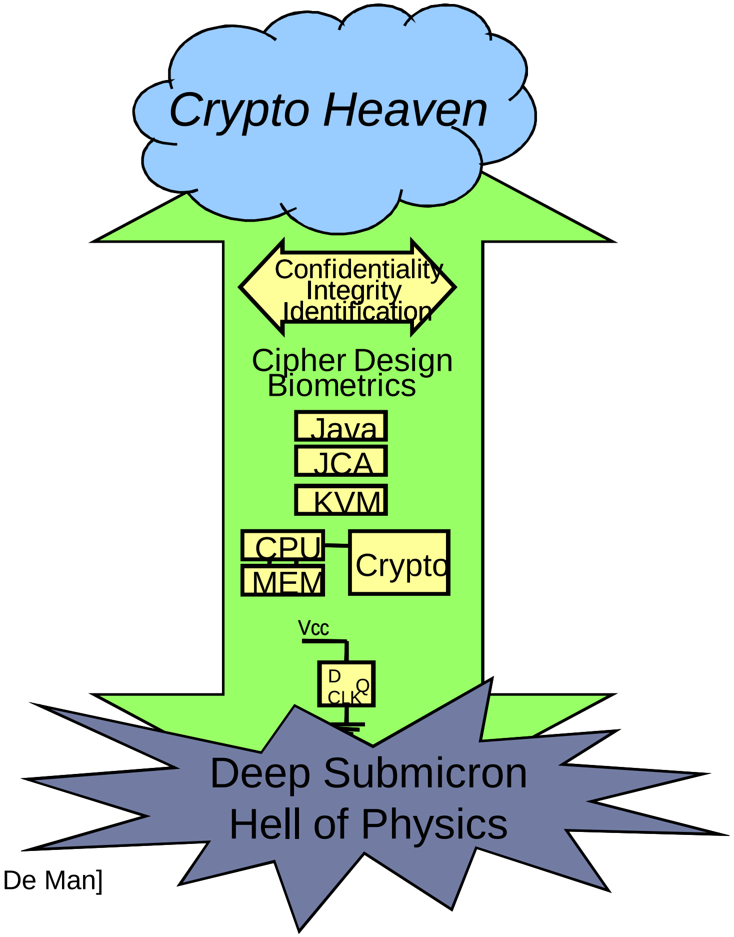
- Security **is not** forever
- Cryptography:
  - Almost all systems from 50 years ago can be broken easily
  - How secure will our current systems in 2059?
- Moore’s law
  - Exponential grow, double each two years
- Technology off the shelf right at hand

Information security principles DOs

- State clear the assumptions
  - GSM: encryption until the base station is sufficient
  - GSM: no need to authenticate the network
  - eID cards: users keep PIN secret
  - RFID: eavesdrop maximum 1 meter
  - Alice has full control on her computer
- Systems are often re-used in scenarios where the initial assumptions do not hold

Information security principles DOs

- Need secure implementations

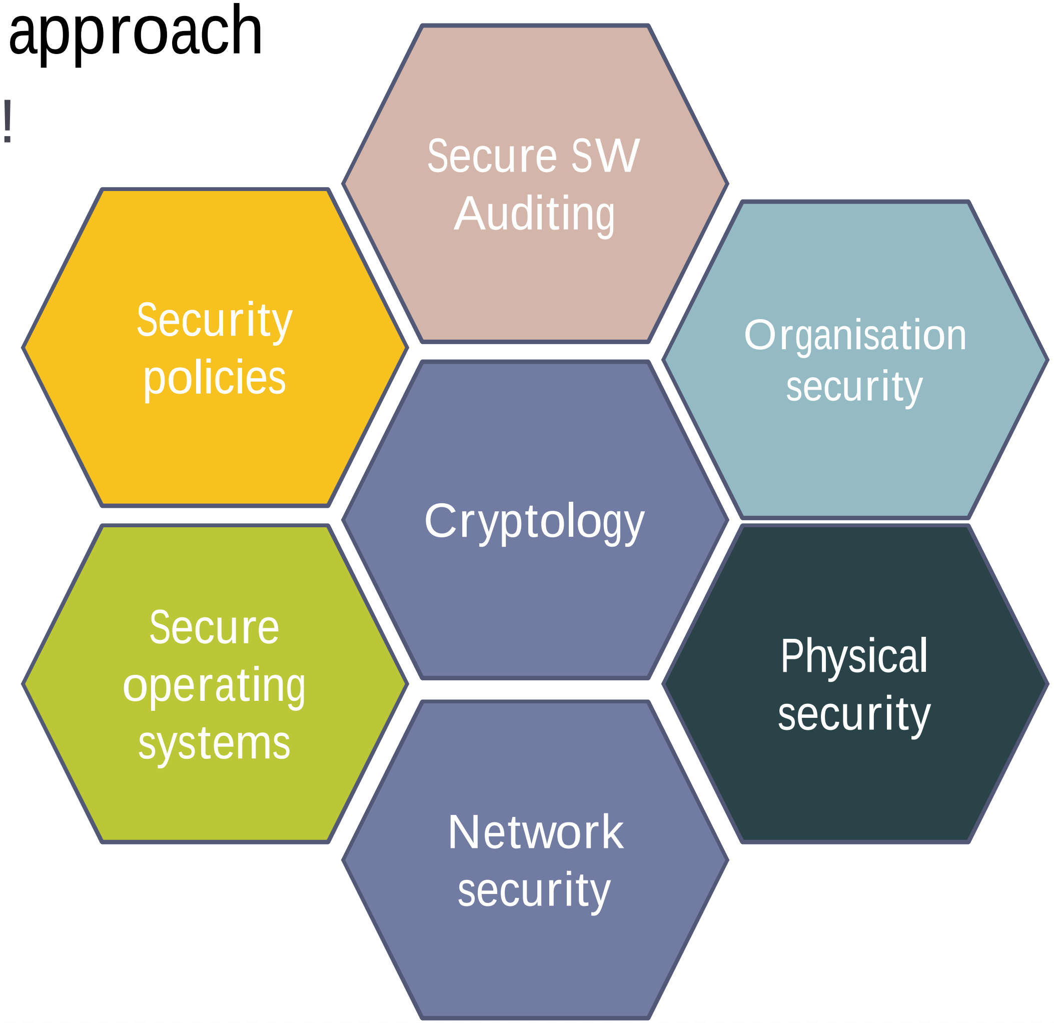


[Modified after H. De Man]

Security is as strong as the weakest link!

Information security principles DOs

- Need for integrated approach
  - Not only technology!
- + legislation
  - DRM
  - Electronic signatures
  - Data retention
  - Liability

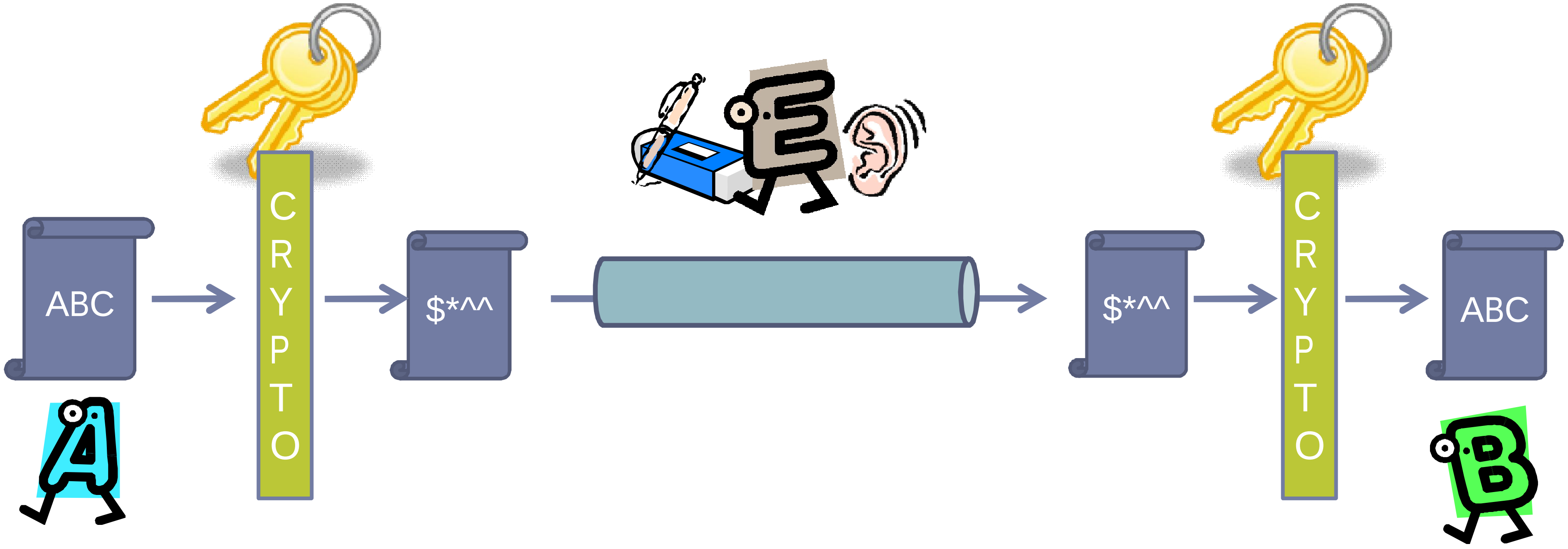


CRYPTOGRAPHY AS A BUILDING BLOCK

Basic building block: Cryptography

"Cryptography refers almost exclusively to encryption, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., ciphertext)"

"THE CODEBREAKERS. The Story of Secret Writing" by David Kahn (1967)



What can E do?

- The scheme is broken if E can deduce the key or recover part of the plaintext

- E can try all keys until obtain plausible plaintext
  - Easy! Long key space

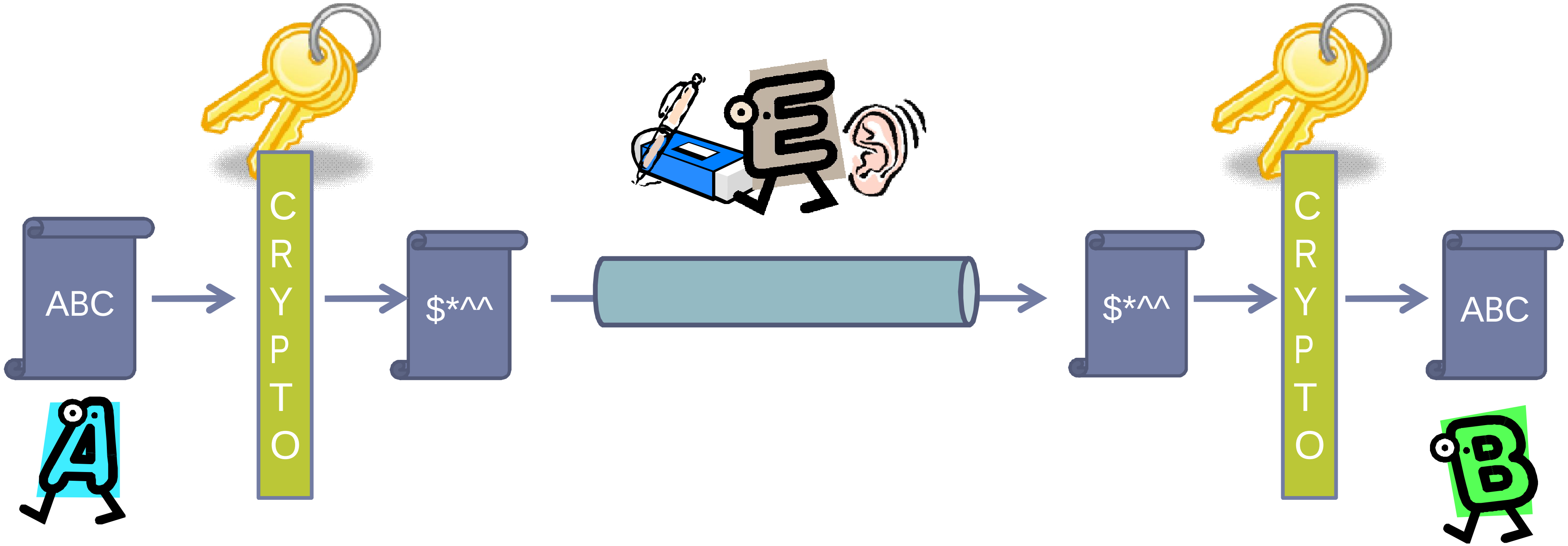
- E try to find shortcuts (faster than brute force)
  - History says E finally wins

- New assumptions:
  - Side channels (timing attacks, power analysis, EM emanations,...)

Symmetric key encryption

- Alice and Bob share keys

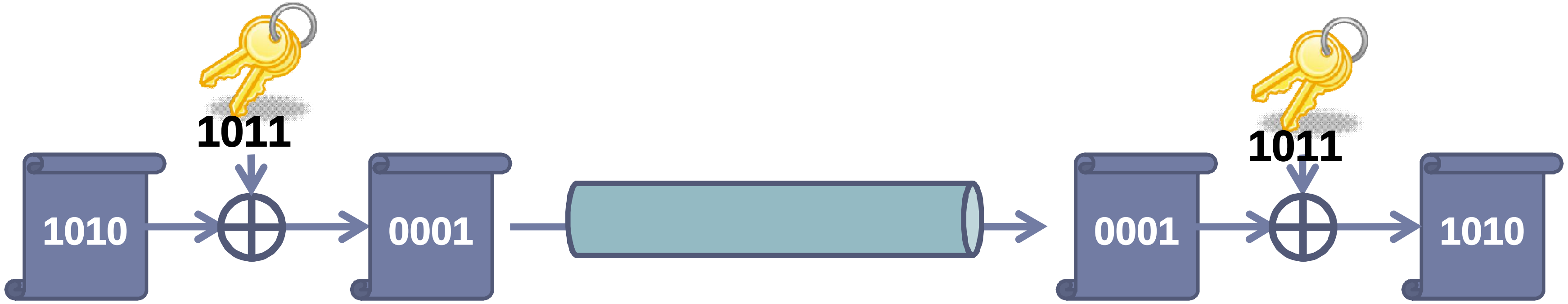
- Achieves confidentiality



Encrypting a message

- Originally permutations and substitutions

- One time pad (Vernam scheme, 1917)



- Do not reuse keys
  - Venona, 1940 - US and UK decrypt Soviet traffic

$$C1 = P1 + K \quad C2 = P2 + K \longrightarrow C1 - C2 = P1 - P2$$

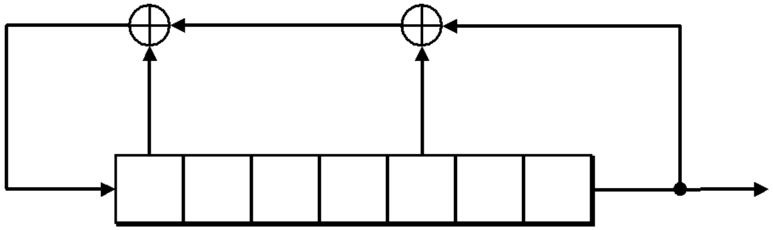
And sadly it is impractical

- 1944–1945, the U.S. Army's broke the one-time pad system used by the Germans because the pads were not completely random — the machine used to generate the pads produced predictable output.

- Needs a key as long as the message. Two options:
  - **Stream ciphers**: create a key as long as the message from a small secret
  - **Block ciphers**: divide the message in small chunks as big as the secret

Stream ciphers

- Generate a random sequence of bits depending on the key
  - Linear Feedback Shift Register (LFSR)

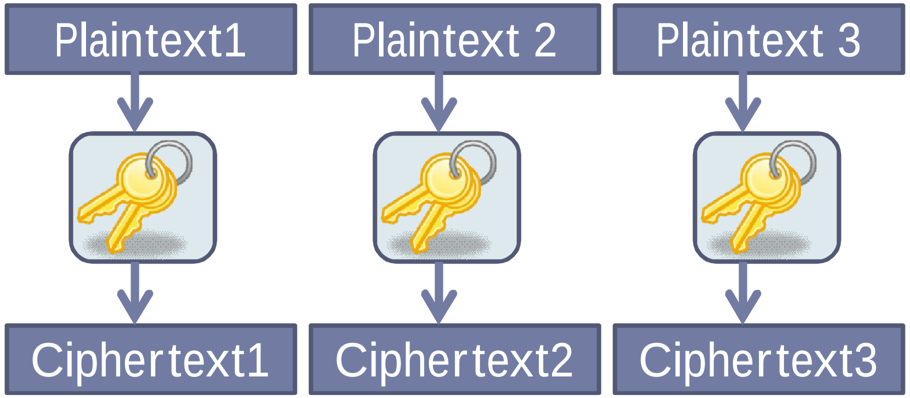


  - Fast
  - RC4, A5/1
  - Need synchronization

  - Difficult to design non-linear LFSR

Block ciphers

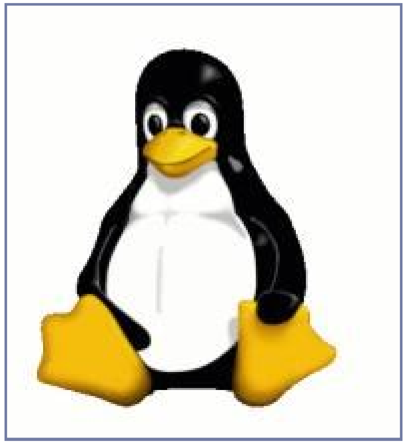
- Encrypts the message divided in fixed-length groups of bits
  - Repeats an operation (round) many times



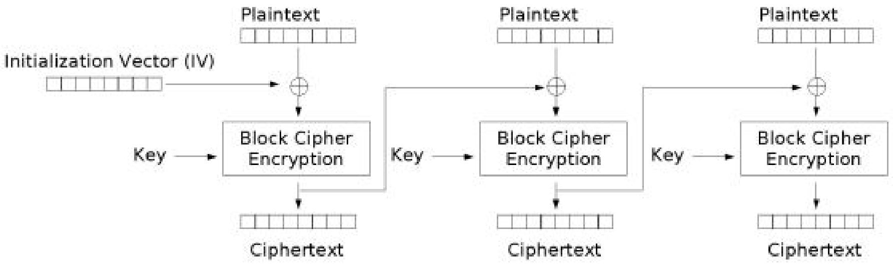
  - Compact in hardware
  - DES, AES

- Encryption modes:
  - Roughly: how to mix the blocks and the key
  - Electronic CodeBook (ECB) , Cipher-Clock Chaining (CBC), Counter, Cipher Feedback CFB, Output feedback OFB,...)

ECB vs CBC

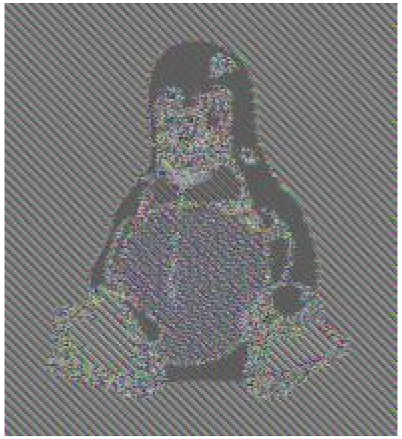


Source: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

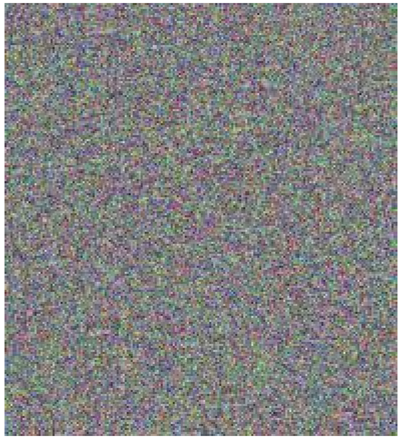


Cipher Block Chaining (CBC) mode encryption

- ECB

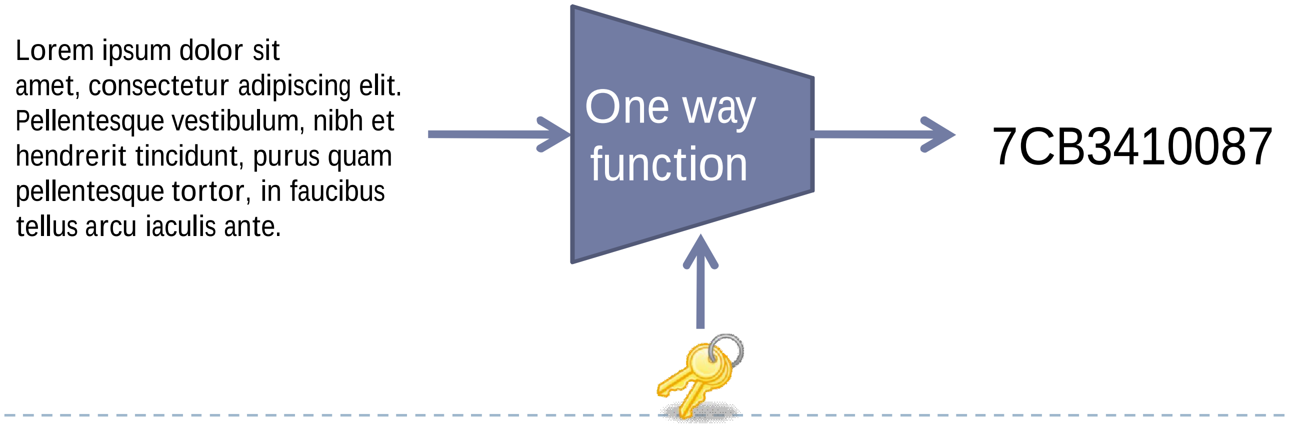


- CBC



Data integrity

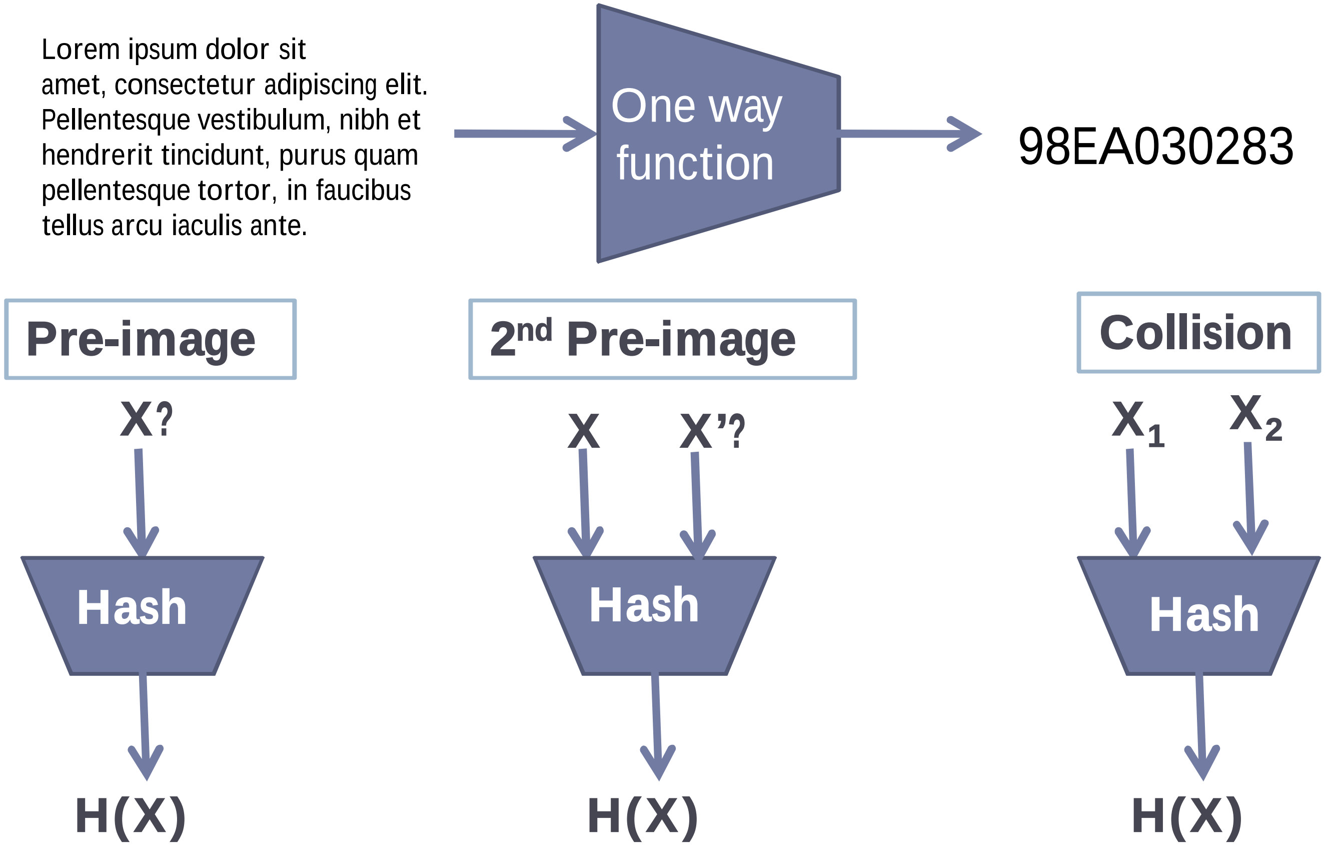
- Encryption does not protect against modifications
- Replace authenticity of long message by authenticity of short string
- Message Authentication Code (MAC)
  - Provides origin authentication



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque vestibulum, nibh et hendrerit tincidunt, purus quam pellentesque tortor, in faucibus tellus arcu iaculis ante.
One way function
7CB3410087

Data integrity

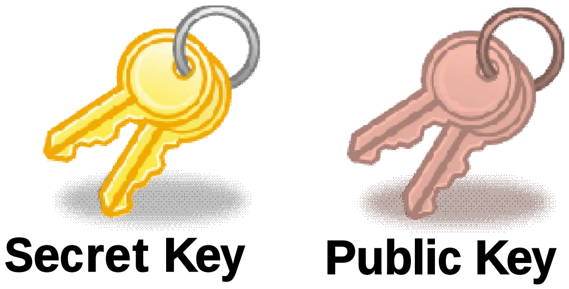
- Manipulation Detection Code (MDC) or Hash function
  - MD5, SHA-1, RIPEMD



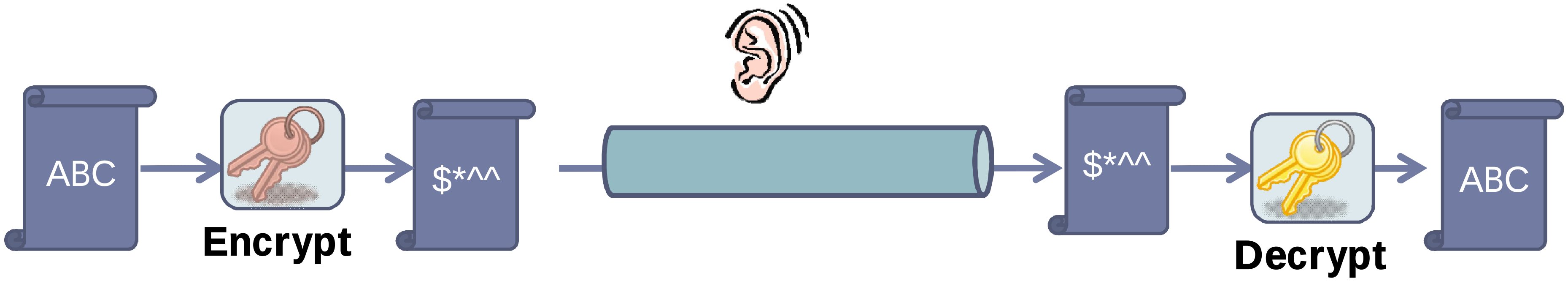
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque vestibulum, nibh et hendrerit tincidunt, purus quam pellentesque tortor, in faucibus tellus arcu iaculis ante.

Public Key Cryptography

- Symmetric key limitations
  - How to establish symmetric keys?
  - How to distribute them?
  - How to store them

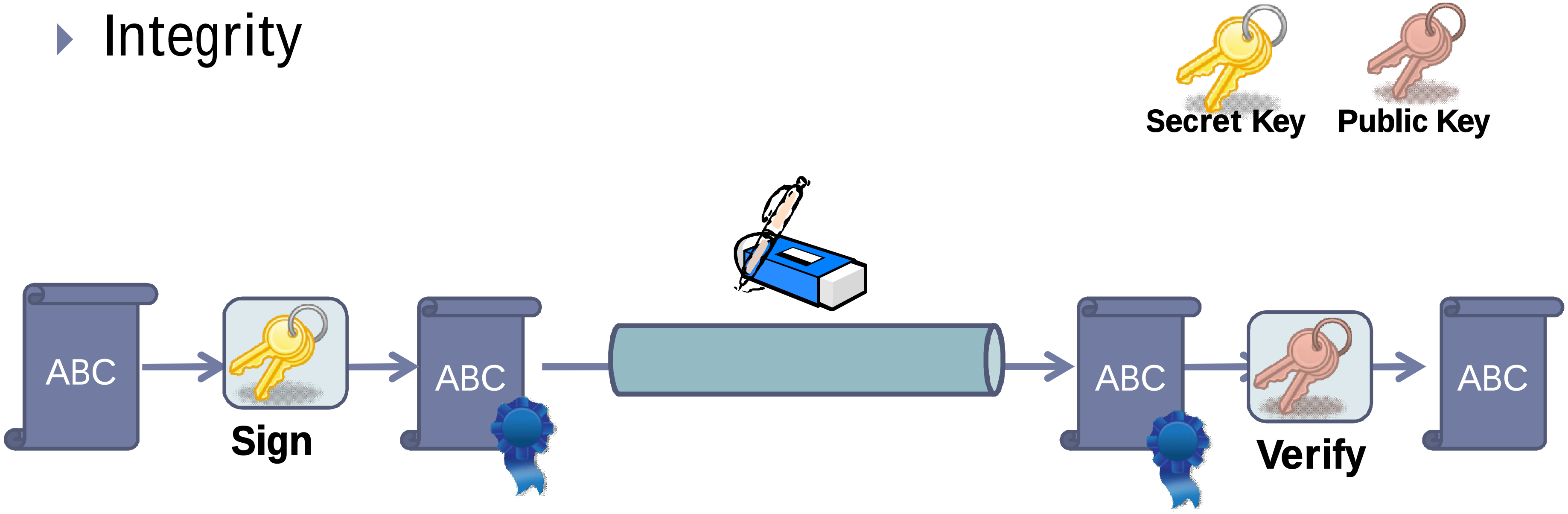


- Confidentiality



Public Key Cryptography

- Integrity



- RSA, ElGamal
- Slow, normally combined with Symmetric Key
  - Key aggreement, another full lecture…

Cryptographic protocols

- Cryptographic primitives combined to perform a security-related function
  - Key agreement
  - Protection against
    - Reply attacks
    - Man in the middle
    - …
  - Anonymity

- **Not** trivial to design!
  - Do not design your own

CONCLUSIONS

Security Engineering

- Security is a property of the overall design
  - You do not get security by using a bit of cryptography or by forcing people to change their passwords frequently
  - Those can sometimes help — but bad guys go around strong security, **not through** (they don't follow rules)
    - To understand how to secure a system, you have to understand what sort of attacks are possible
    - Note necessarily launch them…

- Conflicts:
  - Security versus cost
  - Security versus performance
  - Security versus law
  - Security versus usability
  - Security versus security!

Security design

- The problem is overconstrained
  - Cost, usability, performance, ...

- In the real world, realistic security is often far more important than theoretical security

- What are you trying to protect against whom?
  - Requirements specification is not trivial
  - Neither is to implement them
  - (we'll see more about this tomorrow and thursday)

Humans as users

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations"

Network Security: Private Communication in a Public World (1995)

- Hardest constraint!

Further reading

- R. Anderson, “Security Engineering”
- A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, “Handbook of Applied Cryptography”
- W. Diffie and S. Landau, “Privacy on the line”
- L. Marks, “Between Silk and Cyanide: A codemakers war”