Computer and Network Security

a.y. 2017-18

Prof. Fabrizio d'Amore

damore@dis.uniroma1.it

https://sites.google.com/a/dis.uniroma1.it/cns

Cryptography vs Security

- Cryptography and Security differ
- Cryptography deals with secrecy of information
- Most real security deals with problems of fraud:
  - Message modifications
  - User authentication

- Much of security has little to do with encryption however it might use cryptography
- Almost invariably, encryption does not live alone without some form of *authentication*

Requirements

This course

- ❑Secrecy of communication (encryption)
- ❑Data integrity (how to check if data are modified maliciously)
- ❑Digital signatures (how to sign a digital document)
- ❑Authentication (of user)
- ❑Standard and real world systems
- ❑Availability of…
    - ❑data, computing power, communications media etc.

Encryption: definitions

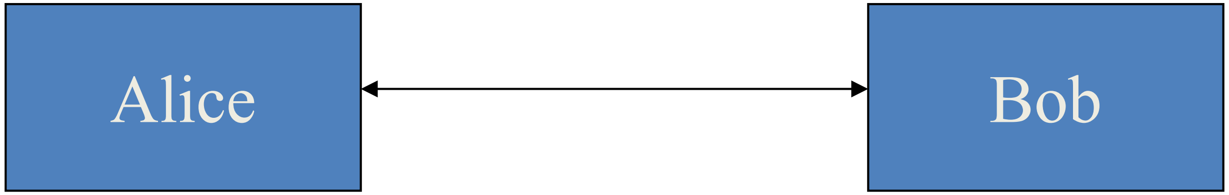
- Encryption function (& algorithm): E
- Decryption function (& algorithm): D
- Encryption key k_1
- Decryption key k_2
- Message space (usually binary strings)
- For every message m: $D_{k2}(E_{k1}(m)) = m$

– Secret key	(Symmetric)	$k_1 = k_2$
– Public key	(Asymmetric)	$k_1 \neq k_2$

Threat & Exploit

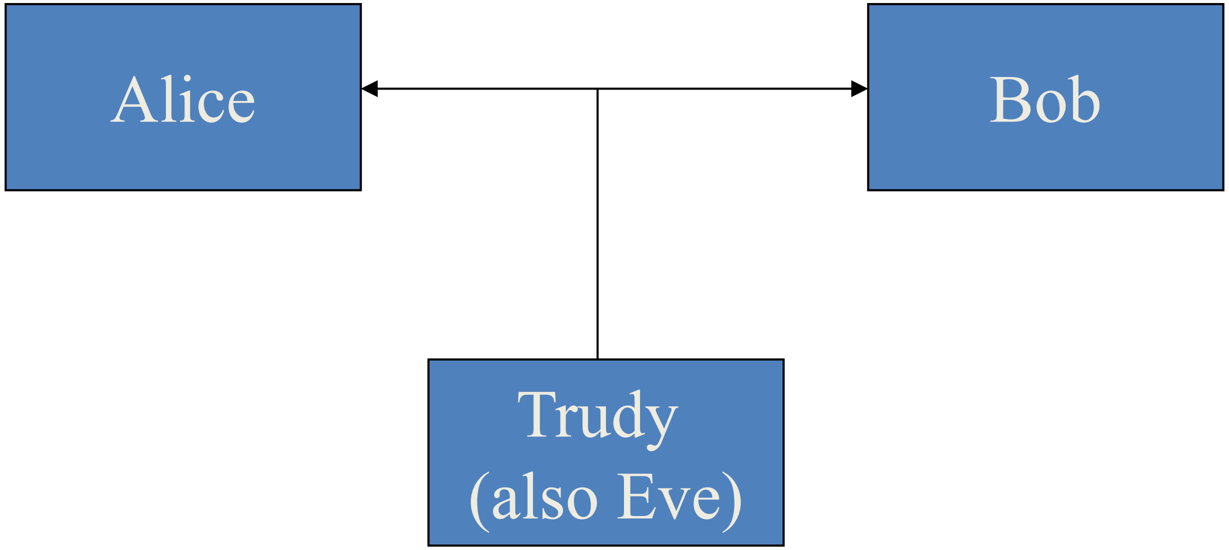
- threat
  - menace, something that is a source of danger
- exploit ("achievement", or "accomplishment")
  - software, chunk of data, or sequence of commands that take advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer (e.g., gaining control of a computer system, allowing privilege escalation, denial of service attack etc.)

Communication Model



1. Two parties – Alice and Bob
2. Reliable communication line
3. Shared encryption scheme: E, D, k_1, k_2
4. Goal: send a message m confidentially

Threat (Attack) Model



4. Goal: send a message *m* confidentially

Adversary

Passive

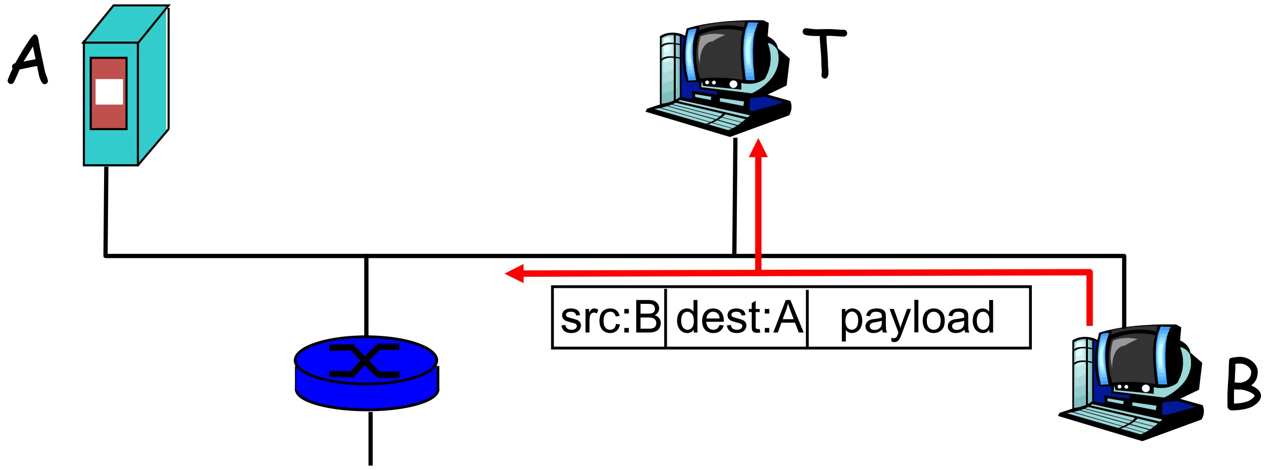
- reads the exchanged messages (no change)

Active

- can modify messages sent by Alice or Bob
- can send false (fake) messages claiming that they have been sent by someone else (Alice or Bob)

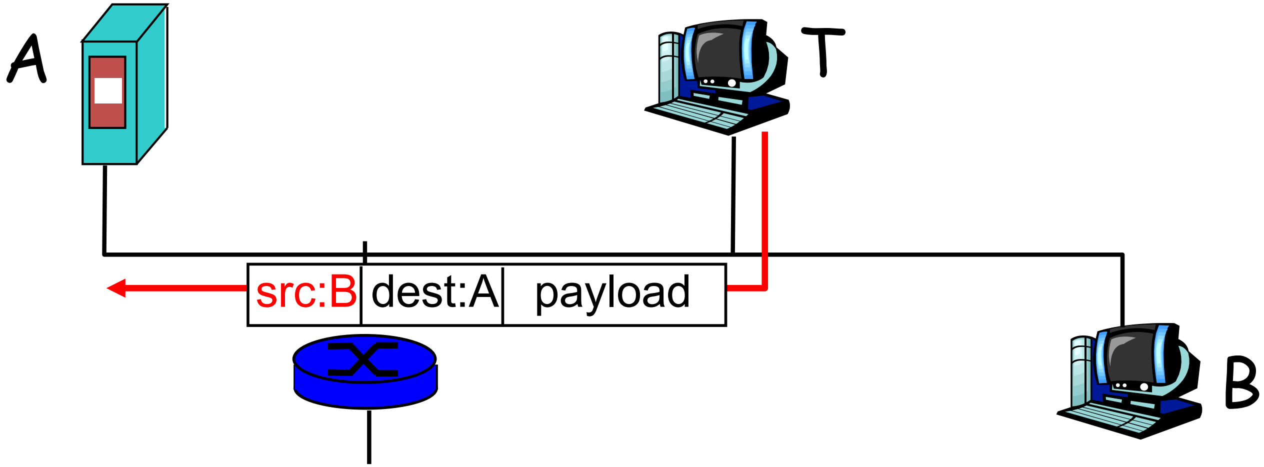
Passive adversary: *packet sniffing*

Trudy reads all messages exchanged by A and B



Active adversary: IP spoofing

T is able to *forge* messages that look like messages sent by B (modification of IP header)

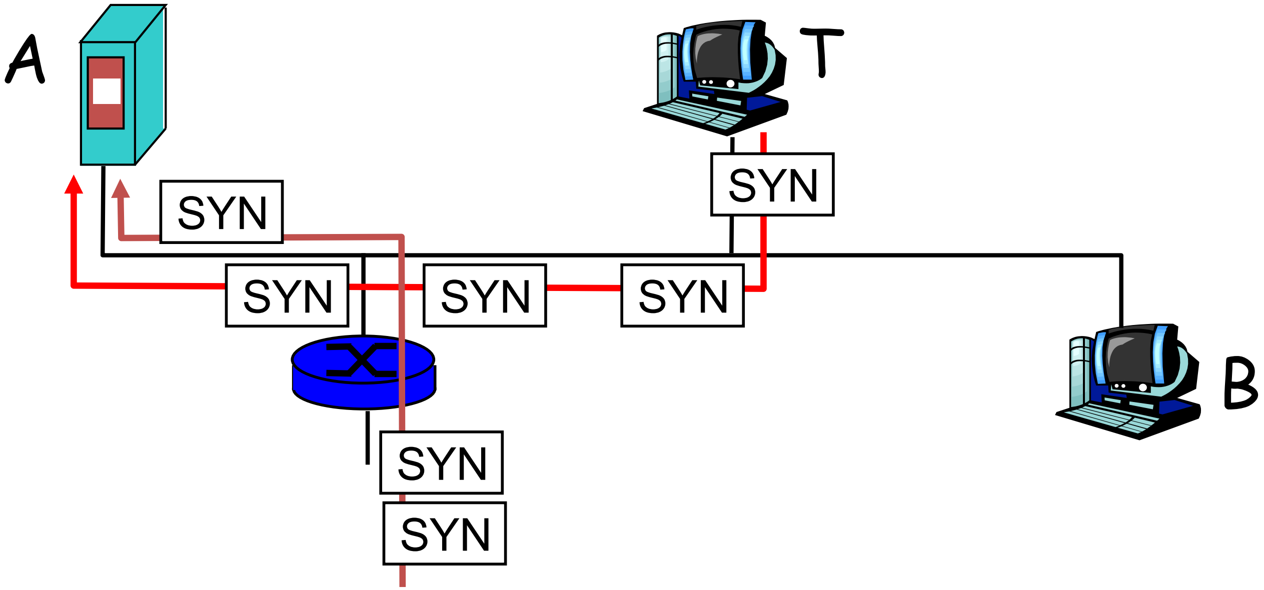


Security Threat: Denial of Service (DoS)

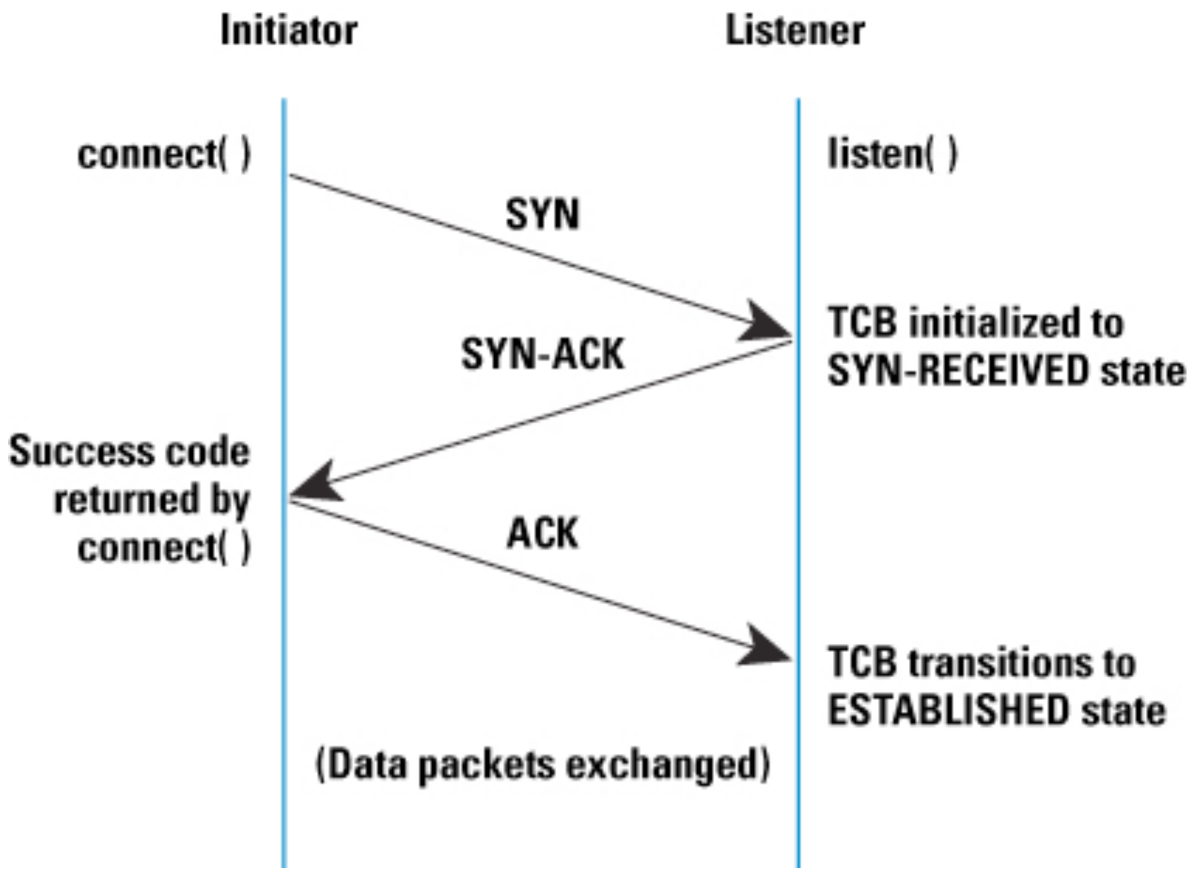
Attackers send many many packets to the attacked host

Distributed attack (DDoS, through infection of unaware computers)

- SYN packets are often used, why?



TCP three way handshake


Initiator
Listener
connect( )
listen( )
SYN
TCB initialized to SYN-RECEIVED state
SYN-ACK
Success code returned by connect( )
ACK
TCB transitions to ESTABLISHED state
(Data packets exchanged)

Security goals

If the keys are unknown then

- it is hard to obtain even partial information on the message
- it is hard to find the key even if we know clear text

HARD = Computationally hard: it takes long time even if the most powerful computers are available

Security goals

Possibilities:

- No adversary can determine message *M (not enough)*
- No adversary can determine some information about *M (not enough)*
- No adversary can determine any *meaningful* information about *M* (*good*)
- *Even in probabilistic sense*

Adversarial model

- Trudy attempts to discover information about M
- Trudy knows the algorithms E, D
- Trudy knows the message space
- Trudy has at least partial information about $E_{k1}(M)$
- Trudy does not know k_1, k_2

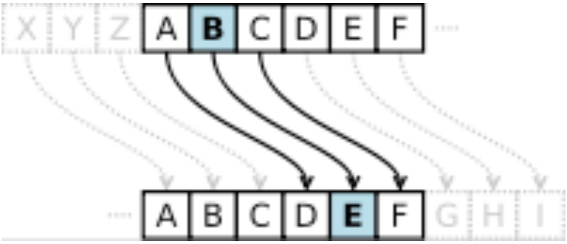
Additional definitions

- Plaintext – the message prior to encryption (“attack at dawn”, “sell MSFT at 57.5”)
- Ciphertext – the message after encryption (“ax4erkjpjepmm”,“jhhfoghjklvhgbljhg”)
- Symmetric key – encryption scheme where $k_1 = k_2$ (classical cryptography)

Examples – bad ciphers

Shift cipher (Caesar’s cipher)

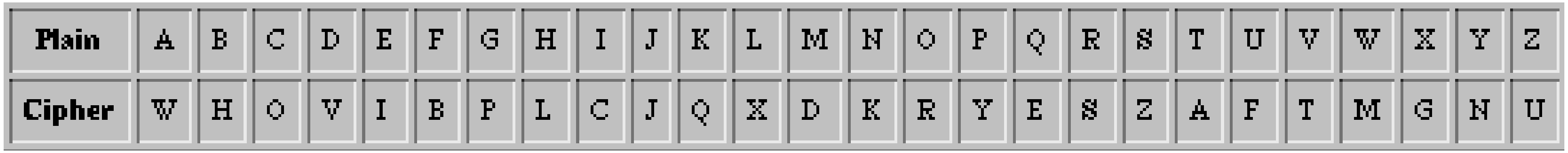
- 26 keys; easy to check them all
- conclusion: large key space required



Substitution cipher

- large key space, but…

Substitution cipher



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

Example

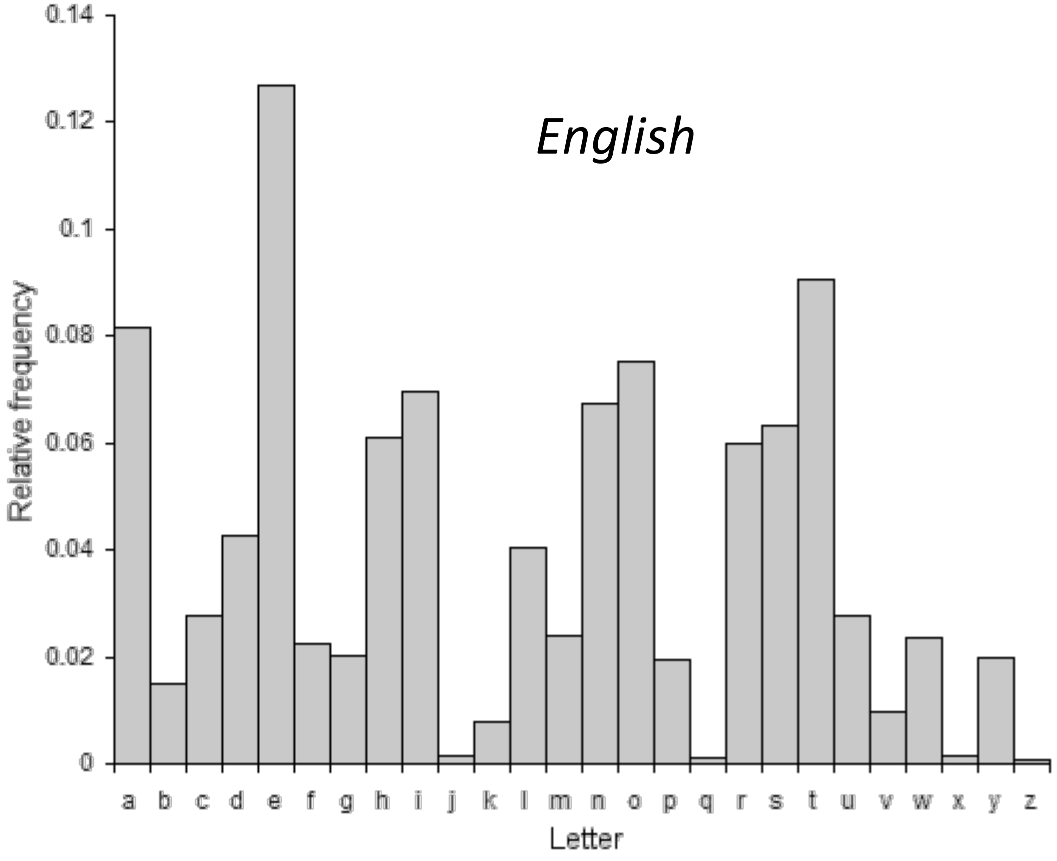
- plaintext: attack at dawn
- ciphertext: waawoq wa vwmk

Size of key space: 26! = 403291461126605635584000000

~ 4.03×10^{26} is it large enough?

Substitution cipher easily breakable

- in spite of huge size of key space, it is still “easy” to break thru statistical analysis of language (frequency analysis)



Perfect Cipher

- Plaintext space = $\{0, 1\}^n$, D known
- Given a ciphertext C the probability that exists $k2$ such that $D_{k2}(C) = P$ for any plaintext P is equal to the apriori probability that P is the plaintext.

In other words: *the ciphertext does not reveal any information on the plaintext*

$\Pr[\text{plaintext} = P \mid \text{ciphertext} = C] = \Pr[\text{plaintext} = P]$
in short: $\Pr[P \mid C] = \Pr[P]$

Probabilities are over the key space and the plaintext space.

Conditional probability

- $\Pr[P \mid C] = \Pr[P \wedge C] / \Pr[C]$ (def. of cond. pr.)
- $\Pr[P \wedge C] = \Pr[P \mid C] \Pr[C] = \Pr[C \mid P] \Pr[P]$ (Th. Bayes)
  - if P and C independent: $\Pr[P \wedge C] = \Pr[P] \Pr[C]$

Hence, in a perfect cipher ($\Pr[P \mid C] = \Pr[P]$):

- $\Pr[P] \Pr[C] = \Pr[C \mid P] \Pr[P]$
- $\Pr[C] = \Pr[C \mid P]$

Example – One Time Pad

AKA Vernam Cipher, invented in 1917 and patented in 1919 while *Gilbert Vernam* was working at AT&T

- Plaintext space: $\{0,1\}^n$
- Key space: $\{0,1\}^n$
- The scheme is symmetric, *key K is chosen at random*
- $E_K(P) = C = P \oplus K$
- $D_K(C) = C \oplus K = P \oplus K \oplus K = P$
- $\oplus$: exclusive OR (bit by bit)

Pros and Cons

- Claim: the one time pad is a perfect cipher. [given a *k* bit cipher text every *k*-bit plain text has got same probability if key is random]
- Problem: size of key space, as show by the following
- Theorem (Shannon): A cipher cannot be perfect if the size of its key space is less than the size of its message space.
- Why???

Proof of Shannon’s th.

- By contradiction.
- Assume #keys (l) < #messages (n) and consider ciphertext C_0 s.t. $\Pr[C_0] > 0$ (C_0 must exist!)
- For some key K, consider $P = D_K(C_0)$. There exist at most l (#keys) such messages (one per each key).
- Choose message P_0 s.t. it is not of the form $D_K(C_0)$ (there exist n-l such messages)
- Hence $\Pr[C_0|P_0]=0$
- But in a perfect cipher $\Pr[C_0|P_0]=\Pr[C_0] > 0$. Contradiction.

Attack Models

- Eavesdropping: secretly listening to private conversation of others without their consent
- Known plaintext: attacker has samples of both plaintext and its encrypted version (ciphertext) and is at liberty to make use of them to reveal further secret information such as secret keys
- Chosen plaintext: attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key

Attack Models

- Adaptive chosen plaintext: the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.
- Chosen ciphertext: the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key.
- Physical access
- “Physical” modification of messages

Computational Power

With sufficient computational power any crypto code can be broken (by trying all possible keys)

- Time
- Hardware
- Storage

When an attack is feasible?

- Theoretical – polynomial time
- Practical (2008) – 2^{64} is feasible, 2^{80} is infeasible (it requires too much time)

Key length

Number of bits of Keys increases over time:

- ***20 bit (1 million keys) easy to break***
- ***56 bit (about 66 million of billion of keys) good 15 years ago: today not safe***
- ***512 bit (more than 40000000….0000000000 - 4 followed by 153 zeri - keys) today: safe; tomorrow?***

Big numbers

Enalotto: different columns	622.614.630=1.15 2^{29}
Seconds since the earth exists	1.38 2^{57}
Clocks in a century of a 3 GHz computer	4.05 2^{61}
Clock in a century of 1000000 2 GHz computers	4.05 2^{81}
249 bit prime numbers of	1.8 2^{244}
Electrons in the universe	1.8 2^{258}

Course outline

- Encryption (secret key and public key)
- Data integrity
- Digital signature
- User authentication
- Randomness, number theory
- Crypotgraphic protocols and standards (SSL, IPSEC, Kerberos, X.509)
- Real world security systems
- Other (??): Watermarking, digital rights management, electronic voting,… ??

Cryptography

- Cryptography is secure communication and
  - Data integrity: how to check whether data have been modified
  - Digital signature: how to sign messages
  - Authentication: how to identify users
- To use it we must define “good” keys: random number generation
- To understand it we need Algebra

Standards

Textbook vs standards

- Robust implementation to attacks
- Combination of several tools in one protocol

Kerberos, SSL, IPSEC, PKCS, X509…

Cryptography vs Security

Cryptography does not guarantee security

- Rules of the thumb Viruses, worms, trojan horses
- Multi level model of security
- Firewalls
- … (depending on time)

Textbook

- *Network Security: private communication in a public world*, 2 ed. Kaufman, Perlman, Speciner, Prentice Hall
- Slides

Other references:

- *Handbook of Applied Cryptography*
  Menezes, Van Oorschot, Vanstone, CRC Press
  download http://www.cacr.math.uwaterloo.ca/hac

- Wikipedia
- Other proposed materials

Slides

Slides on crypto are strongly based on material by Amos Fiat (Tel Aviv U.)

Good crypto courses on the Web with interesting material on web site of:

- Ron Rivest, MIT
- Dan Boneh, Stanford
- Phil Rogaway, Davis
- Doug Stinson, Waterloo
- Amos Fiat, Tel Aviv

SLIDES ARE NOT SUBSTITUTE OF TEXTBOOK !!!!

Exam and office hours

- Written exam
- Office hours: Tuesday 1.30 PM or Friday after class
- E-mail: damore@dis.uniroma1.it
  - No replies to anonymous messages
  - No reply when answer is in Web site
  - Reply: the shorter is the request, the faster will be the reply

Challenge

- ciphertext =

  X R T Z I M L Q S S I R D D R C N N U V F Z U G

- obtained thru the *Vigenère cipher*, a symmetric cipher invented in the XVI century
  - it is a simple polyalphabetic cipher (generalization of the Caesar's cipher)
- plaintext (message) is in English