Informatica ("information électronique ou automatique")

- Si occupa delle informazioni che possono essere
  - Rappresentate (da “informazione” a “dati”)
  - Interpretate (da “dati” a “informazioni”)
  - Conservate (sui computer, solitamente in file)
  - Trasferite
  - Trasformate
- Utilizza i calcolatori (anche detti computer) per effettuare queste operazioni velocemente
  - I computer possono realizzare qualsiasi meccanismo concepibile rappresentando calcoli e senza muovere un singolo cavo (definizione di Dijkstra)

Informazione (in-formare: formare dentro)

- Un’idea formatasi in una mente umana che può essere comunicata attraverso un linguaggio

Algoritmo (dal nome del matematico Persiano Muḥammad ibn Mūsā al-Khwārizmī)

- Una sequenza di operazioni nota ed utile per risolvere una classe di problemi
- Si tratta di una informazione, si trova solo nella mente di chi lo conosce

Programma:

- Una sequenza di istruzioni che un calcolatore può eseguire
- Si tratta di un dato, una rappresentazione di un algoritmo, che può contenere errori (bug)

Network (net – work, lavoro in rete):

- Un gruppo di entità che comunicano (in Informatica, tipicamente computer)

Protocollo:

- Un algoritmo progettato per permettere la comunicazione fra entità diverse stabilendo regole precise per rappresentare informazioni (i messaggi) ed interpretare i dati.
- Presuppone
  - l’identificabilità delle entità (attraverso un indirizzo)
  - la differenza fra le entità in comunicazione
  - la reciproca intenzione di comunicare
  - un canale in grado di veicolare i messaggi
- Esistono moltissimi protocolli di comunicazione: Ethernet, IP, UDP, TCP, 9P2000, HTTP(S) etc..

Internet (International Network)

- Rete mondiale di reti interconnesse
- Basato sul IP (Internet Protocol) e i protocolli basati su esso (TCP, UDP, ICMP, HTTP etc)

Indirizzo IP:

- Indirizzo di un computer su una rete IP
  (IPv4: 1.2.3.4 o IPv6 2001:db8:85a3:0:0:8a2e:370:7334)
- Assegnato da un ISP (Internet Service Provider) o da un server DHCP (Dynamic Host Configuration Protocol)
- Pubblico (unico a livello mondiale) o Privato (unico a livello locale

DNS (Domain Name System)

- Sistema di gestione dei “nomi di dominio”: nomi associati ad un IP

Pacchetto:

- Rappresentazione di una informazione trasferibile su una rete
- Contiene un header (tipicamente contenenti indirizzo, mittente e dimensione)
- Contiene un payload (la rappresentazione dell’informazione che si intende trasferire)

HTTP (HyperText Transfer Protocol):

- E’ il protocollo di comunicazione utilizzato attraverso i browser Web
- Si usa HTTPS per utilizzare un canale di comunicazione criptato.

Attacchi Informatici di base

- MitM (Man in the Middle): Intercettare e/o modificare i dati in transito fra due computer
- DoS (Denial of Service): Impedire ad un computer di ricevere o erogare un servizio
- DDoS (Distributed DoS): DoS basato sulla compromissione di diversi computer per costringerli ad attaccarne uno, sovraccaricandolo ed interrompendo il servizio

One Time Pad (semplificato)

Preparazione:

1. Stabilire l’alfabeto
2. Contare i simboli (= N)
3. Trovare un dado con almeno N facce (o un’altra sorgente random equivalente)

Cifratura:

1. Per ogni lettera (= l) del messaggio
    1. Lanciare un dado (= d)
    2. Accodo il numero alla chiave
    3. Calcolo il resto della divisione (d + l) / N
    4. Accodo la lettera corrispondente al messaggio cifrato
2. Invio SEPARATAMENTE il messaggio cifrato e la chiave al destinatario

Decifratura:

1. Per ogni lettera (= l) del messaggio cifrato
    1. Prendo la lettera corrispondente della chiave (= c)
    2. Calcolo il resto della divisione (N + l – c) / N
    3. Accodo la lettera corrispondente al messaggio decifrato