La Steganografia

Marin Riccardo
Esami di Stato 2017/2018 | 5^TEL B
ISIS A.Malignani - Udine

Perchè la steganografia?

- Evoluzione di Internet → Cresce l'importanza dell'informazione

Perchè la steganografia?

- Evoluzione di Internet → Cresce l'importanza dell'informazione

Steganografia

Crittografia

Privacy

Libertà espressione

Introduzione

Steganografia $\rightarrow$ steganòs (nascosto) + gràphein (scrivere)

Introduzione

Steganografia → steganòs (nascosto) + gràphein (scrivere)

- Tecnica che permette di nascondere un messaggio segreto in un messaggio pubblico

Servizi

→ Confidenzialità

→ Integrità

→ Autenticazione

→ Non ripudiazione

→ Identificazione

Crittografia vs steganografia

- Crittografia → mira a rendere incomprensibile un messaggio, tranne al destinatario

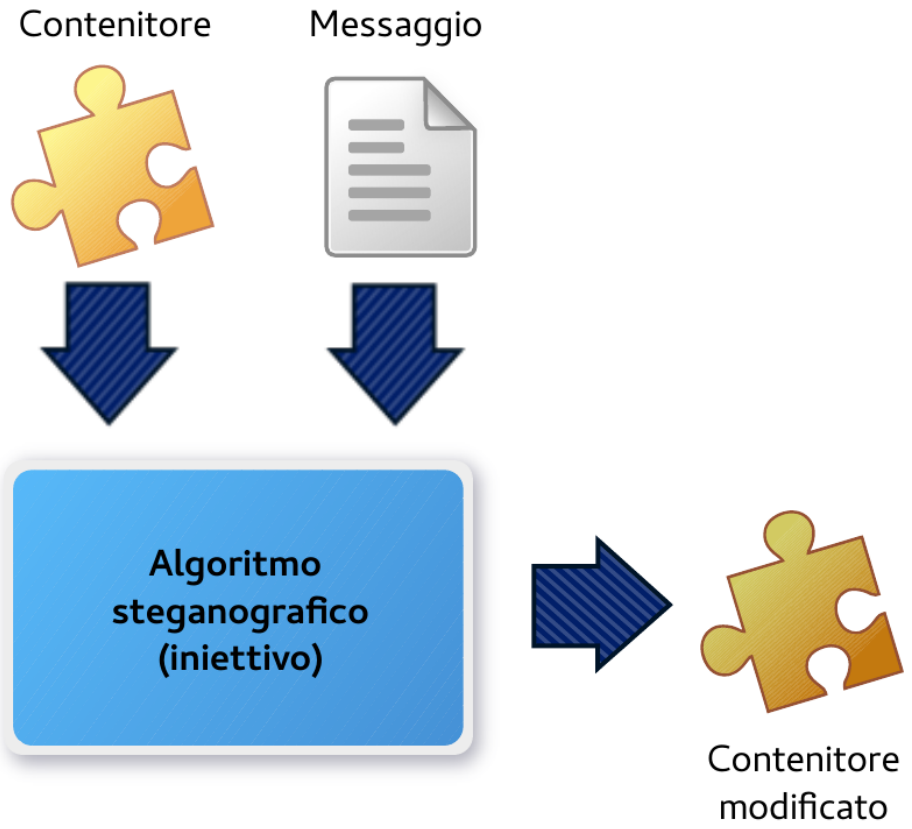
  Fallisce quando l'attaccante decripta/ricostruisce il messaggio originario

- Steganografia → nasconde l'esistenza stessa del messaggio

  Fallisce quando l'attaccante capisce che c'è un messaggio nascosto

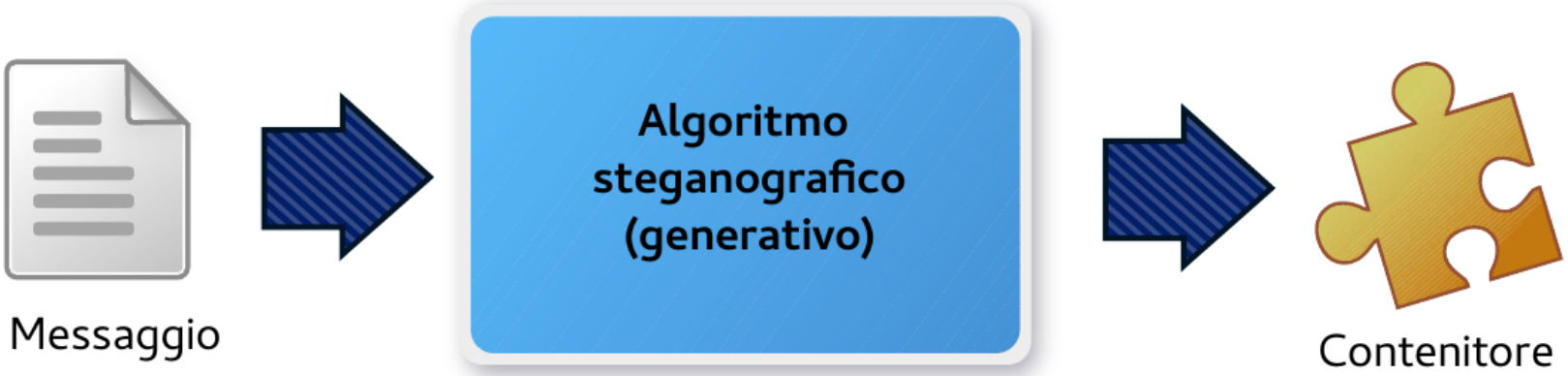
Modelli steganografici

- Iniettivo



Modelli steganografici

- Generativo



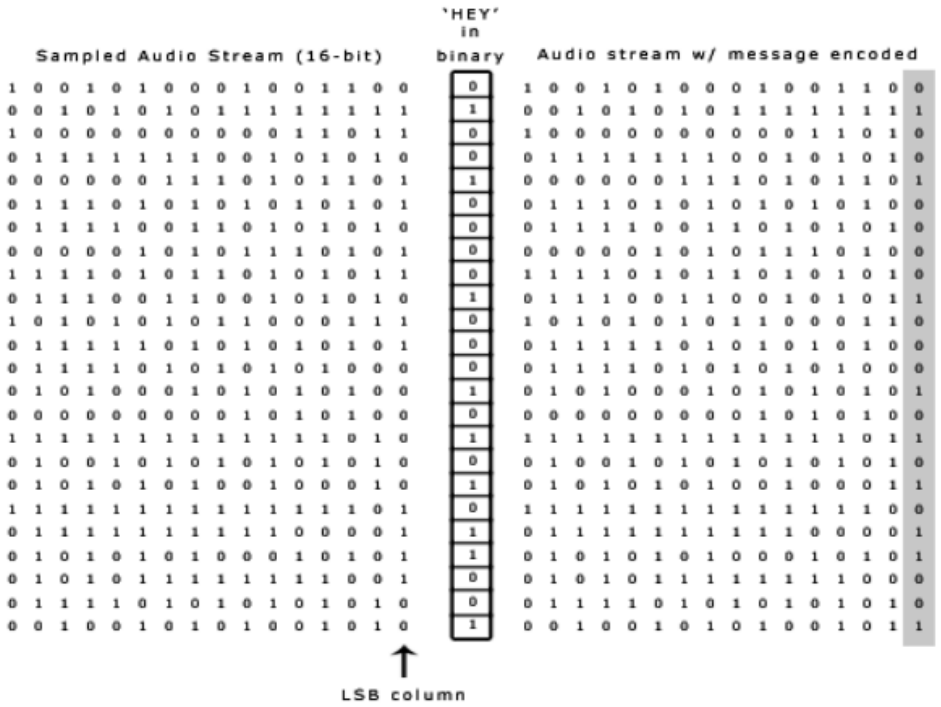
Steganografia nei testi

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Pershing sails from NY (r) June 1

Steganografia audio

- Codifica LSB
- Codifica di parità
- Codifica di fase



Steganografia immagini

- Dominio spaziale → altera direttamente i pixel

- Dominio delle trasformate → immagine scomposta in coefficienti, poi modificati

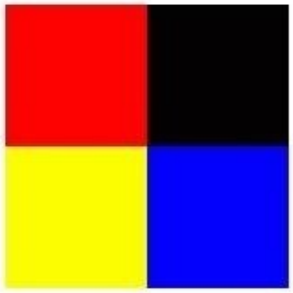
Steganografia immagini

Original Image

```
11111111  00000000
00000000  00000000
00000000  00000000

11111111  00000000
11111111  00000000
00000000  11111111
```

Stego Image



```
11111101  00000011
00000010  00000001
00000000  00000010

11111100  00000011
11111101  00000001
00000001  11111100
```

c	a	t
01 10 00 11	01 10 00 01	01 11 01 00

Applicazioni

- Watermarking/fingerprinting
- Terrorismo
- Libertà di parola

Steganalisi

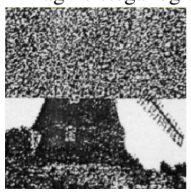
- Attacco visuale

Immagine contenitore

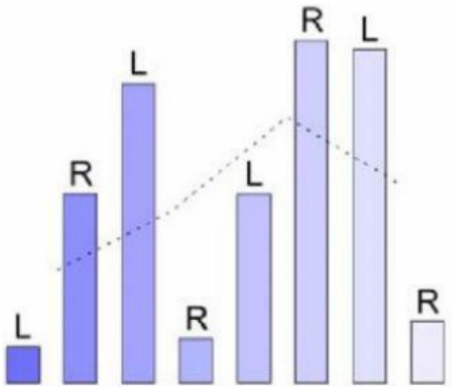
Immagine steganografata al 50%

Immagine contenitore filtrata

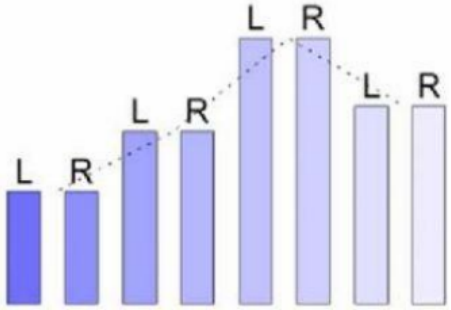
Immagine steganografata filtrata



- Attacco statistico



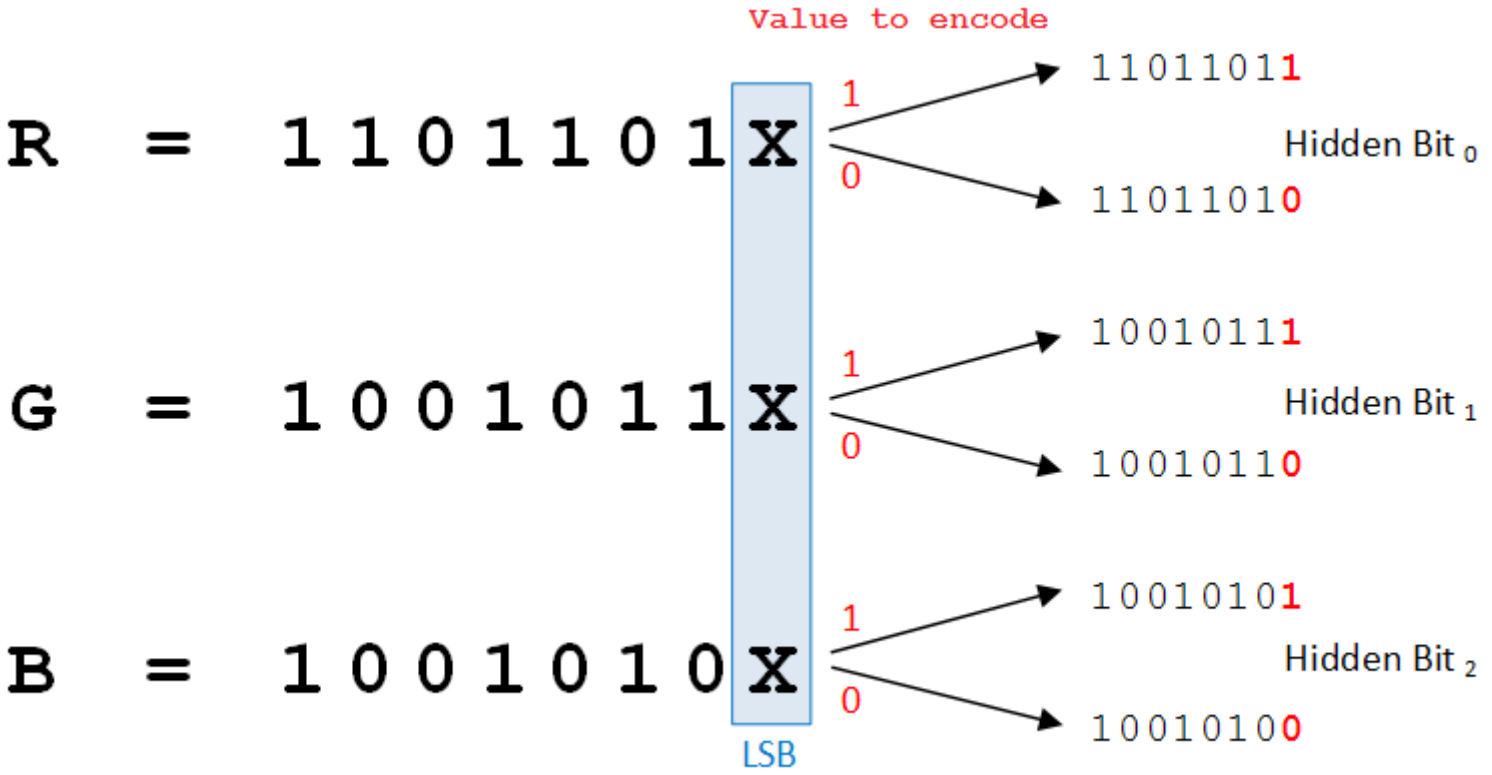
Freq. colore prima



Freq. colore dopo

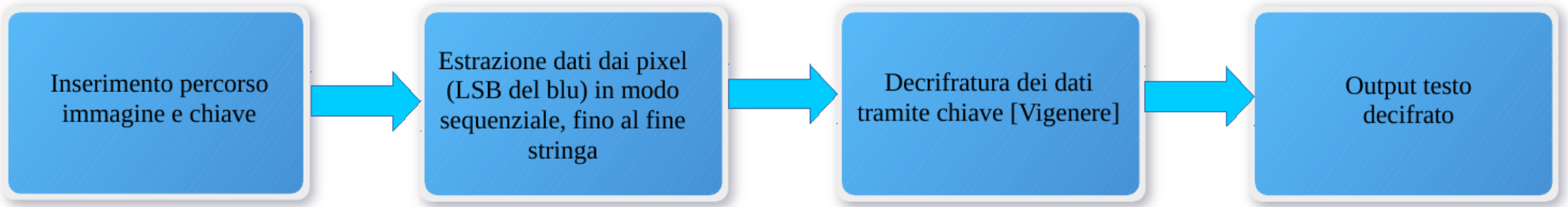
StegoMalignani

- Steganografia LSB su immagini BMP



StegoMalignani

- Schema a blocchi



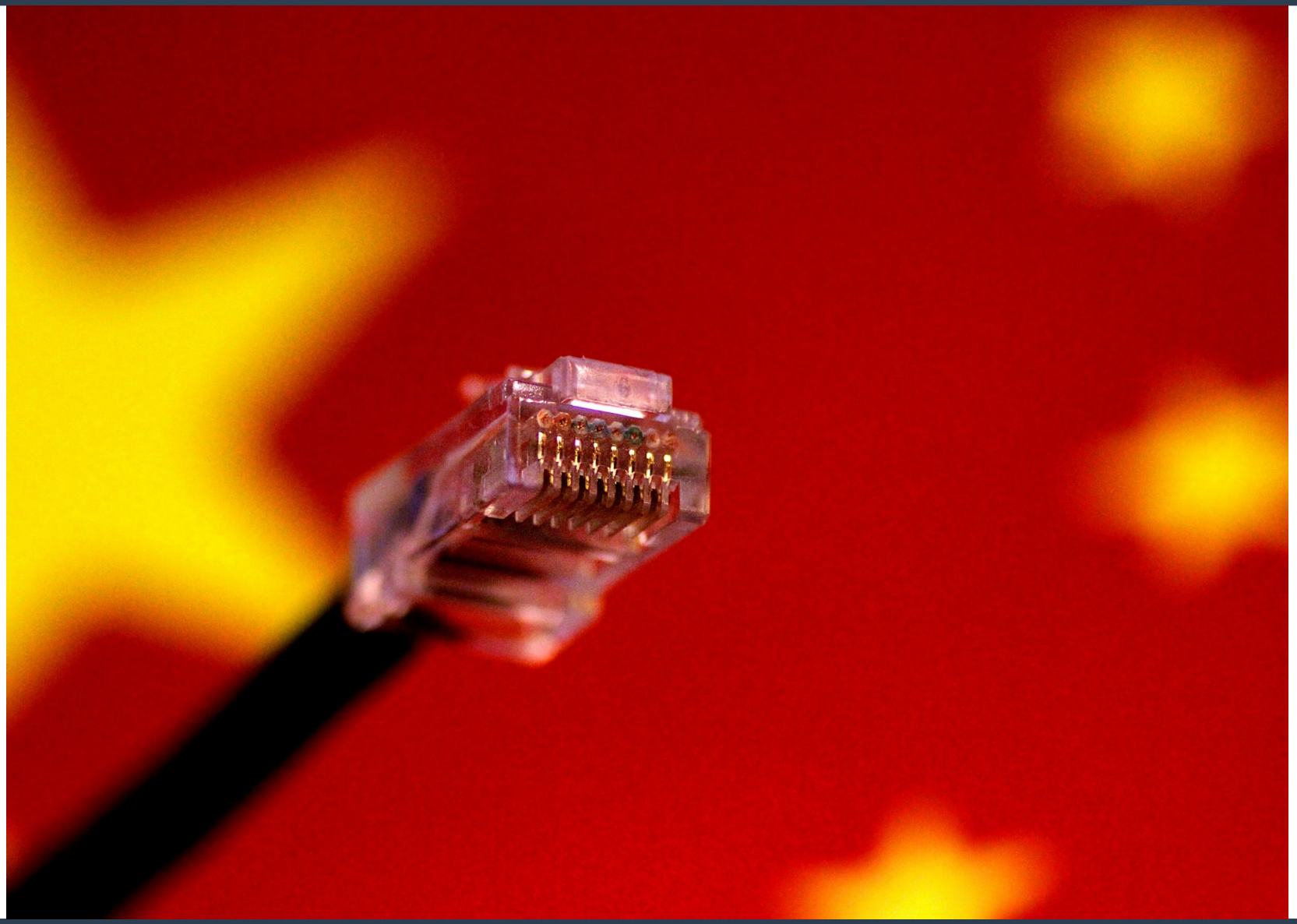
StegoMalignani

- Unisce steganografia e crittografia

- Criteri di segretezza:

  → Genericità
  → Diffusione
  → Unicità

The Great Firewall of China



Brief history

- 1949 → People's Republic of China (Mao)
  - Land distribution
  - Harsh actions against opposition

Brief history

- 1949 → People's Republic of China (Mao)

  - Land distribution
  - Harsh actions against opposition

- 1976 → Deng Xiaoping

  - Economic reforms, open market
  - But also blocking Western ideas

Brief history

- 1989 → Tiananmen Square protest

Brief history

- 1989 → Tiananmen Square protest

- 1998 → Golden Shield Project

  - Network security
  - Great Firewall of China (censorship)

Brief history

- 1989 → Tiananmen Square protest

- 1998 → Golden Shield Project

  - Network security
  - Great Firewall of China (censorship)

The Great Firewall

- Control of the exit node of China and ISPs

The Great Firewall

- Control of the exit node of China and ISPs

Internet filtering:

- Block specific domain names or ip addresses
- Keyword censorship
- VPNs detection

Forbidden websites and services

- Politic dissent, Tibet and Xinjiang independence
- Religion, sexual content, violence, gambling

I don’t agree

Constitution rules

Migration

Winnie the Pooh

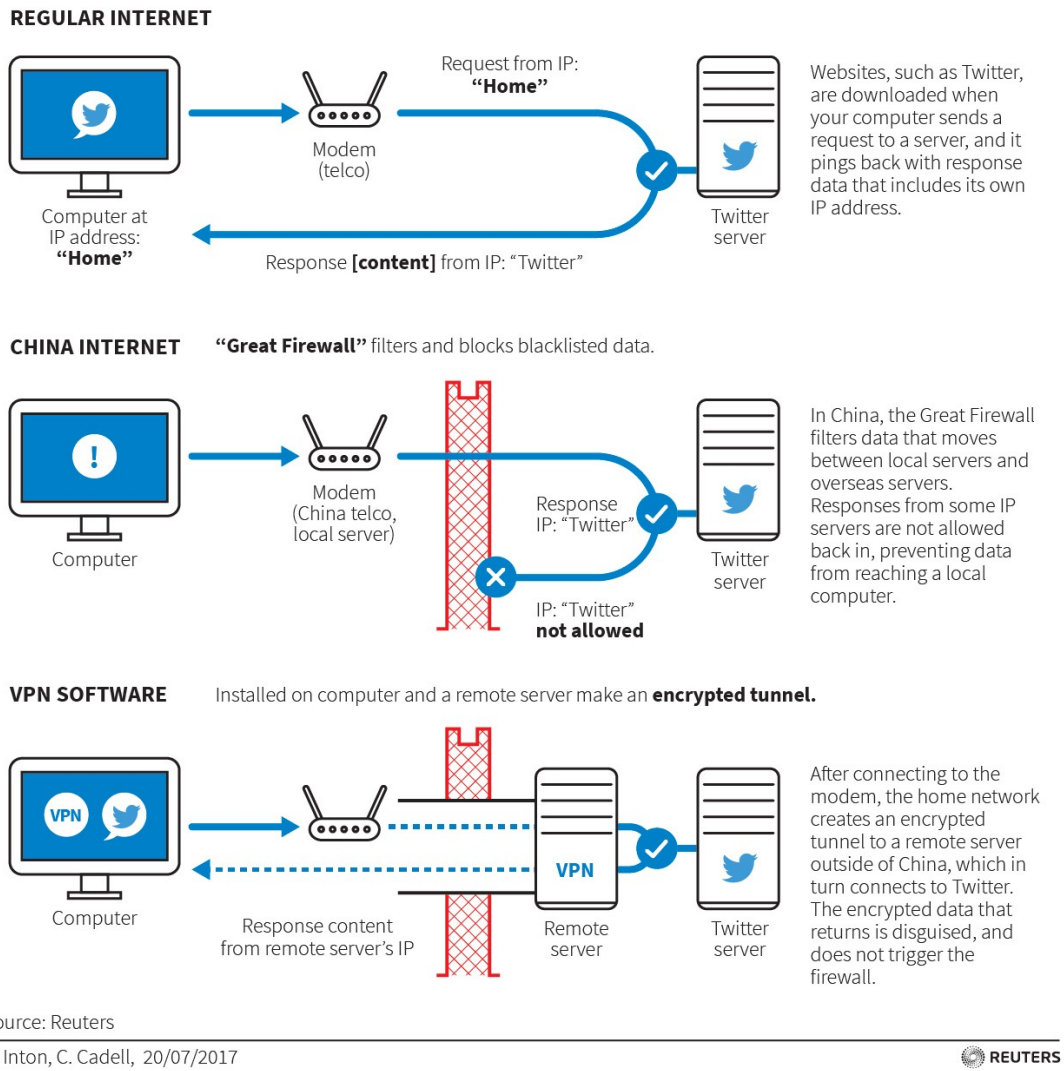
Bypass the GFW

- Proxy

  Traffic rerouted through proxy servers

- VPN

  Encrypted tunnel



Reasons

- Social impact

Reasons

- Social impact

  - Internal traffic (to Chinese servers)

  - Self-censorship

Reasons

- Economical impact

Reasons

- Economical impact

  - Trade protectionism

  - Chinese version of foreign web giants

Reasons

- Foreign reactions

  - American companies provided hardware and software (es. Cisco)

  - Controversy for human rights violations

Conclusions and future prospects

- Internet → tool that can bring democracy

- In China authoritarianism rises with development of technology

The perfect totalitarian dystopia?