

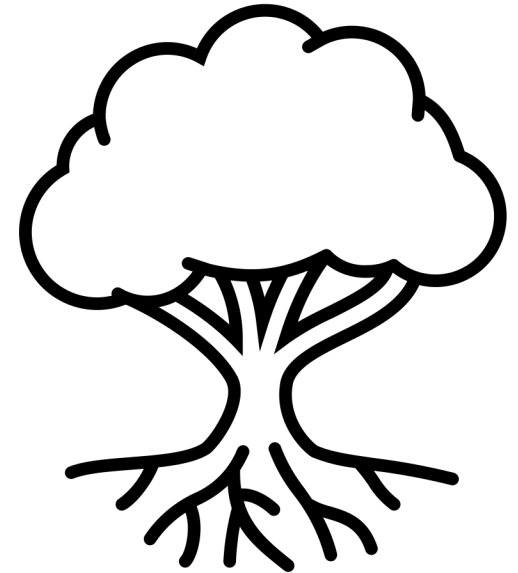
Historiskt sammanhang

Del av kursen ETE352 Cybersäkerhet - grunder och medvetenhet
som ges vid Linköpings universitet

Mikael Asplund

Cybersäkerhetens rötter

- Hemlig kommunikation (före 1900-talet)
- Digitala koder och maskinkryptering (Under 1900-talet)
- Datorvirus (1980 och framåt)
- Internetbaserade attacker (2000-talet)



Hemlig kommunikation

- Tidigt militärt behov
- Steganografi - Konsten att gömma meddelanden
- Kryptografi – Meddelandet är inte gömt, men dess mening är det
 - Chiffer



Maria Stuart

- Skottlands drottning 1542-1567
- Fångslad av sin kusin Elisabeth I
- Konspirerade för att mörda sin kusin (Babington plot)
- Breven krypterades men knäcktes
- Maria avrättades 1587



Maskinkryptering

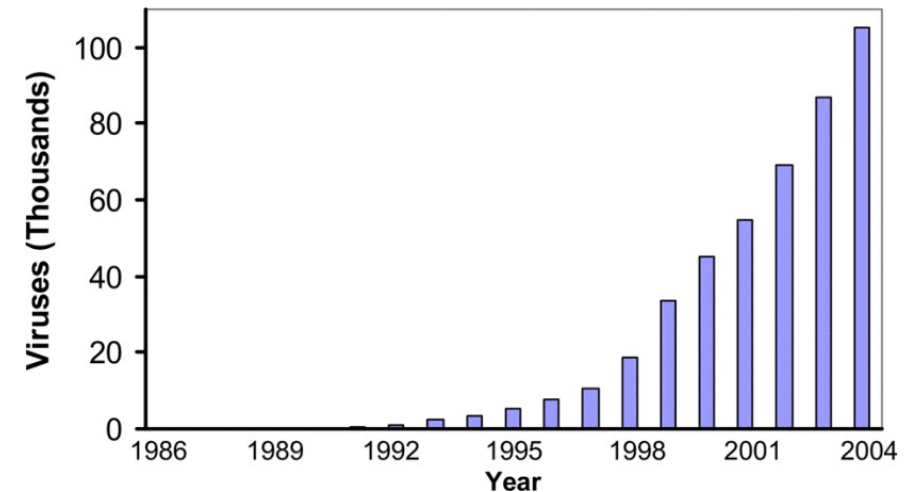
- Under 1900-talet blir elektronisk kommunikation dominerande
- Ökande komplexitet på chiffer och matematiken för att knäcka dem
- Enigma – Avancerat krypteringssystem som ändå kunde knäckas



Datorvirus

- 1971: Creeper – en mask i ARPANET
- 1982: Elk Cloner
- Dramatisk ökning av virus och dess negativa effekter under 90 och 00-talen

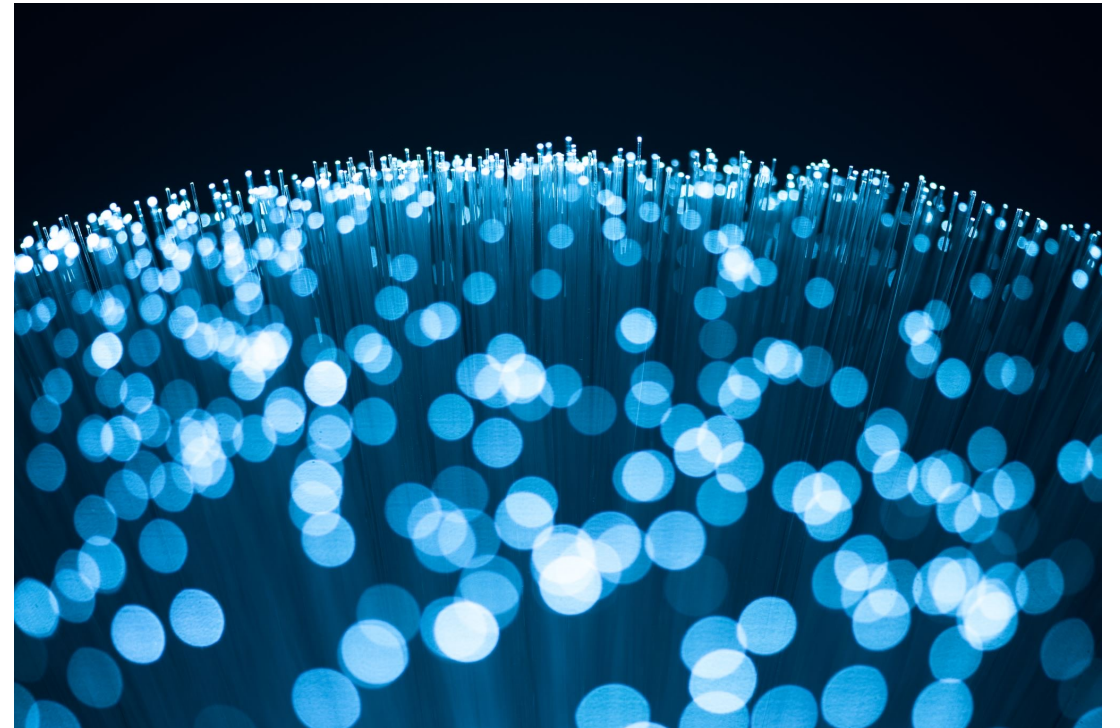
```
ELK CLONER:  
  THE PROGRAM WITH A PERSONALITY  
  
IT WILL GET ON ALL YOUR DISKS  
IT WILL INFILTRATE YOUR CHIPS  
YES IT'S CLONER!  
  
IT WILL STICK TO YOU LIKE GLUE  
IT WILL MODIFY RAM TOO  
SEND IN THE CLONER!  
  
□
```



[10.1109/RAMS.2008.4925840](https://doi.org/10.1109/RAMS.2008.4925840)

Internetåldern

- Dataintrång blir enkelt
- Spam blir lönsamt
- Webb och mejl blir attackytor
- Början av 2000-talet: fortfarande begränsad omfattning



<https://cybersakerhet-grund.ida.liu.se>