ICOM 5018

Network Security and Cryptography

Description

This course introduces and provides practical experience in network security issues and cryptographic techniques. Cryptographic algorithms and protocols are introduced and their use in secure protocols such as secure shell (SSH) and secure mail (Pretty Good Privacy/PGP) are studied.

Topics

- **Conventional encryption, algorithms and techniques**
- **Public key cryptography and a little number theory**
- **Authentication and hash functions**
- **Digital signatures and authentication protocols**
- **Electronic mail, IP, and web security**
- **The cryptographic techniques used in intruders, viruses, and worms**
- **Firewalls**
- **Cryptanalysis methods and methods of exploiting protocol weaknesses**
- **Legal and social issues – current legislation**

Instructor – *Thomas L. Noack* (details at-amadeus.uprm.edu/~noack/crypto)

Projects – Many possibilities – protocol weaknesses, interdisciplinary

Prerequisites – *ICOM 5007 and INEL 4307 or permission of instructor*

What crypto does

- Confidentiality
- Authentication
  - Signature – is this the only copy
  - Content verification – did someone modify
  - When was this signed – still valid
- Individual identification at a distance
  - Key distribution – with a key server
  - Key agreement – mutual agreement, no global server

Where you see it

- Commercial transactions
  - Internet and electronic purchases
  - Electronic fund transfers and the money laundromat
- Medical and other data
  - Privacy of medical records
  - But getting insurance benefits

Other privacy applications

- Data security and authentication
  - Personnel and payroll records
  - Individual files on a server
  - Controlled database access – you can see your info –
- Intellectual property protection
  - DVDs, Music, eBooks, movie content
- System login and passwords

The components of crypto

- Private key crypto
  - Key must be kept secret
  - Separate key for each group of users
- Public key crypto
  - Knowing public key doesn’t reveal private key
  - Can be used for secrecy or authentication

More components

- Hash and message authentication
  - Message digest – long message, short authenticator
  - Saves encryption effort
  - One-way function – only encrypted password is stored
- Key exchange
  - You can agree on a key without having a trusted key distributor

Some basic principles

- Don’t use secret or amateur algorithms
  - The crypto community tries to break the published algorithms – if they haven’t, you can trust them a bit more
  - Algorithm strength should depend only on key length alone – known method, nearly unguessable key
  - Again, don’t invent your own – read the literature and understand the problems and weaknesses

What we study - principles

- **Conventional encryption, algorithms and techniques**
- **Public key cryptography and a little number theory**
- **Authentication and hash functions**
- **Digital signatures and authentication protocols**

What we study - applications

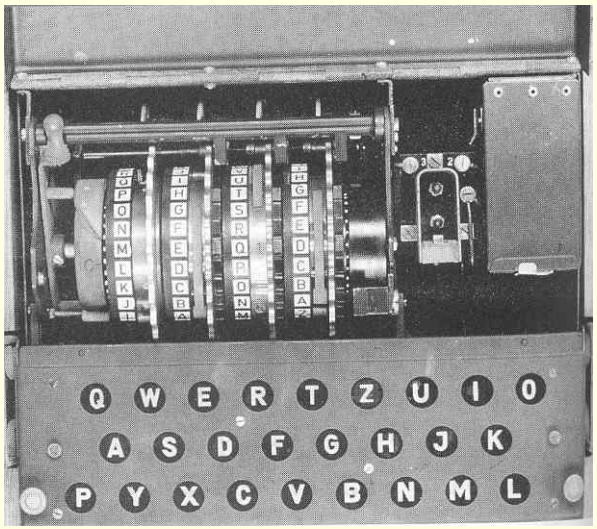
- **Electronic mail, IP, and web security**
- **The cryptographic techniques used in intruders, viruses, and worms**
- **Firewalls**
- **Cryptanalysis methods and methods of exploiting protocol weaknesses**
- **Legal and social issues – current legislation**

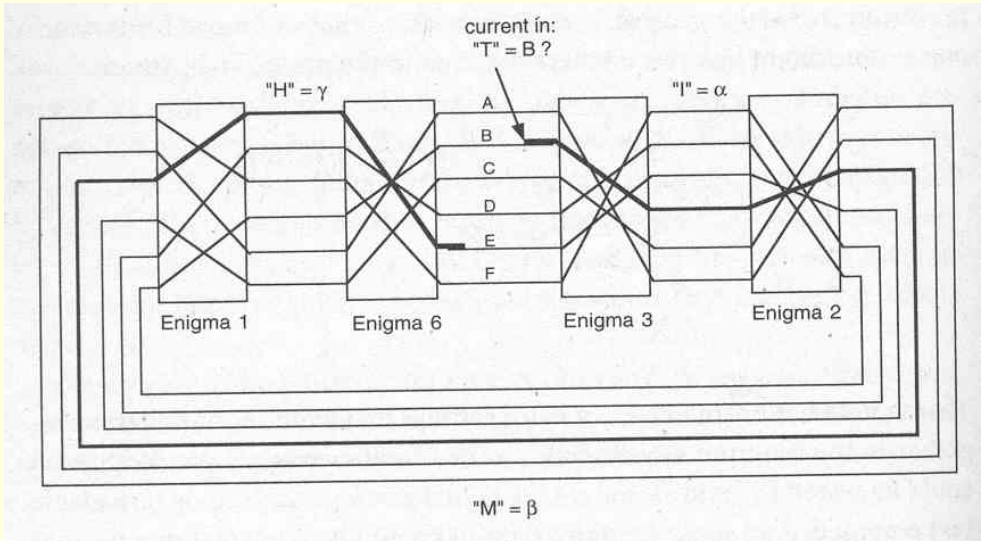
What are the difficult parts

- Studying the weakness of systems and protocols
  - Historically, and now, little procedure weaknesses and subtle traps have changed history
- Understanding how attacks work
- Understanding how it fits together
  - Complete systems include browsers and outside systems over which you don’t have control – crypto is global, just like the internet

The 4-rotor Enigma, with wiring

pictures from Budiansky, Stephen, *Battle of Wits*

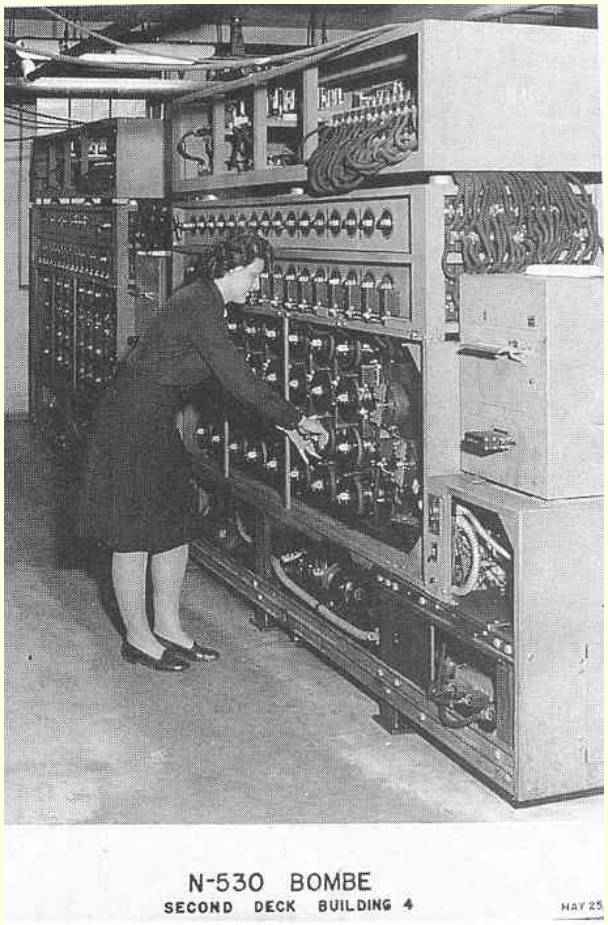




Uses the polyalphabetic principle

- Repositioning the rotors gives a new alphabet
- The rotors are stepped at each character
- It was broken at least partly because of operator carelessness

The *Bombe* , used to break Enigma messages



picture from Budiansky, Stephen, ***Battle of Wits***

Comments

- This is actually a copy of the machine conceived by Turing
- It still used a plugboard approach rather than a strictly electronic stored program
- Material captured from ships and submarines was also used
- This was a combination of known plaintext and brute force cryptanalysis
- It is not a Turing machine in the computer science sense