Between Silk and Cyanide

An Intro to cryptography, and why it applies to you.

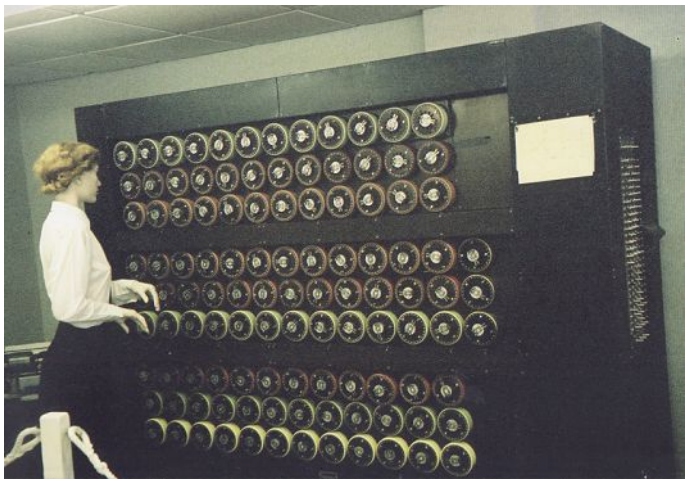
Julia Freeman http://quixotic.eu/

Early Beginnings

- First cryptography system credited to the Spartans – Scytale
- Mentioned in the Kama-Sutra – mlecchita-vikalpa – Art of secret writing
- Julius Caesar in the Gallic Wars – Caeser Cipher
- Mary Queen of scots
- Vigenère Cypher – Sixteenth century
- Mechanisation – Enter Babbage
- World war one – ADFGVX, The Zimmerman Telegram
- The modern age of crypto...

Bombes, Bletchly & Bombs

- All previous ciphers had a short key length to ciphertext length.
- If the key is as long as the cipher text, it is uncrackable (In theory)
- Enter the enigma



I told you once

- The only system that is 100% secure is the one time pad
- Relies on random number generation
- But how do you distribute Keys?

Standards, love 'em

- US seeks to create a new standard for digital encryption
- Adopted 1976 – Data Encryption Standard
- Had 56bit key. Rumoured to be knobbled by the NSA
- 56bit key didn't last long, may as well use Welsh.
- Improved with 3DES
- Later replaced with Advanced Encryption Standard - AES

Helpful Hippy

- AES, 3DES, all suffered from one problem
- Key Exchange
- First solved by Whitfield Diffie & Martin Hellman
- Diffie-hellman Solved it
- Not the tidiest solution, but it gave hope

Manischewitz is the answer

- First discovered by Ronald Rivest after a Passover Party with some students
- Published by Ronald Rivest, Adi Shamir and Leonard Adleman
- Called RSA
- Based on one way mathematical functions and large prime numbers
- Public Key Cryptography is born.

P & Q & E & N

- The maths of it all:
- p and q are large prime numbers, and kept secret
- p and q multiplied together gives us N
- e is another large prime number
- e and N together consist of the public Key, p and q the secret key
- d is calculated using Euclids algorithm and the second equation

$$C = M^e (\mathrm{mod}\ N)$$

$$e \times d = 1 (mod(p-1) \times (q-1))$$

$$M = C^d (\mathrm{mod}\ N)$$

Prove it

- Key exchange solved
- Secure if using a big enough key
- Does rely on secure random numbers
- A whole new world of possibilities arises
- Can be used for proof of sender, as well as encryption

Got a license for that T-Shirt?

- RSA was rapidly classified as a munition by the US
- Electronic export of RSA illegal
- Enter Phil Zimmerman
- Pretty Good Privacy provides for ubiquitous cryptography.
- Arrest Phil Zimmerman
- Release Phil Zimmerman
- Never say no to a geek

A wilderbeast at this time of night?

- PGP was good, very good
- It wasn't however “free”
- GNU implement PGP (in canada) and release under the GPL
- Strong Encryption is now free for everyone to enjoy.
- What has this got to do with you?

You did what with the fish?

- Why do I need crypto?
- I have done nothing wrong so have nothing to hide
- RIP
- Vulnerable to Rubber hose cryptanalysis

What do I do about it?

- Generate a key
- Distribute the key
- Sign and be signed
- Use it

Find out more

- The Code Book – Simon Singh – ISBN-9781857028799
- Applied Cryptography – Bruce Schnier – ISBN 9780471117094
- Secrets and lies – Bruce Schnier – ISBN 9780471453802
- Beyond Fear – Bruce Schnier – ISBN 9780387026206
- The art of deception – Kevin Mitnick – ISBN 9780764542800
- Cryptogram – Bruce Schnier - Monthly newsletter

Make it so!

- Any Questions?

Euclids Algorithm

```
int gdc(int a, int b)
{
    return (b == 0 ? a : gcd(b, a % b) );
}
```