Why are we doing this?

PGP/Gpg is free/libre Public Key

Community solution

- web of trust not hierarchy
- Trust as emergent property

Why is that good?

Crypto Machines thru History

- scytale (rhymes with Italy) BC
  - transposition

- Magic decoder disks
  - And strip equivalents
  - centuries
- Adding machine – offline, letter substitution
  - Not just Enigma
  - decades

- Teletype xor PRNG – bauds, online
- Computers – recent decades

Using Enigma

Kinds of Ciphers

Substitution

Transposition

Compound

Cipher Implementations

Mental – Pig Latin, Rhyming Slang, Navajo Code-talker

Pencil

Pencil & Reference

Disks or Strips

Mechanical (adding machine tech) offline

Electro-Mechanical (baud scrambling with mechanical cycle) online

Computer

Key

- Symmetric or Shared Secret
  - Traditional
  - Key distribution problem – out of band transmission
  - Trust the chain of custody
- Asymmetric, Public Key
  - late 20th Cent
  - Still has a private secret key but not shared
  - Chain or web of trust

Secret Keys subtypes

- Short, repeating
- Long, reused
- Short, generating nearly infinite
- Nearly infinite, random – One time pad
  - Loses security if ANY reuse
  - VENONA
- Nearly infinite, pseudo random
  - If PRNG sequence doesn't leak sequence definition

Public Key niche

- Exquisitely expensive to use for encrypting even moderately large messages
- Only actually used for
  - Authentication
  - Key distribution - encrypting a nonce random number, used to key fast symmetric cipher
- Authenticity of Public Keys is bootstrap problem
  - Hierarchy of Trust resting on security of a few root keys (Verisign CA cert in browsers)
  - Community web of trust – keysigning party

Modern Substitution Algorithms

Most secure if text *etc* compressed first
- Destroy statistics

Stream ciphers
- pure substitution at char or bit level
- Bit transposition is byte substitution

Block ciphers – block substitution
- Keyed reversible mixing of input bytes in block
  - typically Feistel structure of iterated mixing rounds
- padding for small data
- 'Modes of Operation' for larger data
  - http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation
- Hybrid if viewed at byte or bit level

One Time Pad

- Multiple discovers, multiple uses
  - Vernam Mauborgne, 1917-1919, teletype tape first!
  - Post ww1 (into WW2)
    - super-encipherment pads
    - German Foreign Office & USSR dip, GRU/KGB
  - WW2
    - Marks/SOE & GCCS/BP pads
    - SIGSALY voice, Sturgeon tape
  - Coldwar
    - Shannon proof
    - SIGTOT & Hotline
    - pads in Cuban stores on Grenada
    - Pocket OTP – Unix, Brit Forces

http://en.wikipedia.org/wiki/One-time_pad

Unbeakable?

Theory *vs* Practice

Implementation flaws

Public Key

Moore's lap, time = factors

Software bugs

Session key protected, but is session cipher safe?

Block Ciphers

computationally, practically

Software Bugs

Sophisticated structural & statistical attacks

OTP

Russians and Germans dupped One Time Pads in WWII (VENONA, GEE)

German GEE OTP mechanically non-random

Machine key-stretching

computationally, practically

Indicator group / Nonce key

Complications can be simplifications

On-air training with simplified procedures

Slowly tightening practice

Cribs and Collisions

Detecting two *text* messages in same key

```
LQSQC YDGMK EHEAG PCKMY EGOBS HUNBK GJTSU
LQSQL CTSMP MRTMV BLZGI RAXWW KVZGL PBDFY

UQYPC XZLJE ARVBU ADVEH GCJTR MUQZT LB
WGTXW DXLRK KQGYH SWPCH GCBSG SOSDT W

NOTEA LSOTH ATTHE WHOLE RANGE IDEAI SRATH
NOTET HATTR DOESN OTDOR EGULA REXPR ESSIO

ERUNP ORTAB LEBET WEENC HARAC TERSE TS
NCHAR ACTER CLASS ESSUC HASDO RLOWE R
```

Higher Collision rates detect synchronized key-streams. Even detects reuse of aperiodic keys. Putting two or more in depth will cancel key, allow riffing

Defense = Compress
no more or less common chars, chars no longer forced to byte align so 'depth' hader

Crib – start is easiest but can drag

Cribbing works with any key system ... if trial key can be extended which can signal if crib was matched for real.

For more information

Free libre content http://en.wikipedia.org/wiki/Cryptography
http://en.wikipedia.org/wiki/Wikipedia:WikiProject_Cryptography#Free_content

- Infosecpedia (old: GFDL new: Creative commons)
- The GNU Privacy handbook (GFDL)
- PlanetMath article on Cryptography and Number Theory (GFDL)
- Cracking DES (public domain, apart from a couple of chapters which reproduce published papers)
- NIST documents on Cryptography, mostly the FIPS standards
- Greg Goebel'sCodes, Ciphers, & Codebreaking — public domain.
- CryptoDox — crypto wiki licensed under the GNU Free Documentation License

Further reading

http://en.wikipedia.org/wiki/Cryptography#Further_reading

Handbook of Applied Cryptography by A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone CRC Press, (PDF download available), somewhat more mathematical than Schneier's Applied Cryptography.

Introduction to Modern Cryptography by Phillip Rogaway and Mihir Bellare, a mathematical introduction to theoretical cryptography including reduction-based security proofs. PDFdownload.

Cryptonomicon by Neal Stephenson (novel, WW2 Enigma cryptanalysis figures into the story, though not always realistically).

A Cryptographic Compendium http://www.quadibloc.com/crypto/intro.htm

More

http://planetmath.org/encyclopedia/CryptographyAndNumberTheory.html

Bletchley http://www.tnmoc.org/home.aspx

http://www.schneier.com/paper-self-study.html Self-Study Course in Block Cipher Cryptanalysis

Matthew D. Russell (2004-02-27). "Tinyness: An Overview of TEA and Related Ciphers". Archived from the original on 2007-08-12.
http://web.archive.org/web/20070812222155/http://www-users.cs.york.ac.uk/~matthew/TEA/
.

http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Authenticated encryption modes: CCM | CWC | EAX
http://en.wikipedia.org/wiki/EAX_mode | GCM | OCB

http://en.wikipedia.org/wiki/Disk_encryption_theory

Image Credits

http://www.w1tp.com/enigma Museum

Wikipedia.org & WikiMedia Cc-by-sa

- http://en.wikipedia.org/wiki/Portal:Cryptography