Cryptography: A brief history and its importance for cyber security

Chris Mitchell
me@chrismitchell.net
www.chrismitchell.net

Agenda

1. Crypto – a (very) selective history
2. Crypto – its role in cyber
3. Challenges
4. The future

Agenda

1. Crypto – a (very) selective history
2. Crypto – its role in cyber
3. Challenges
4. The future

Cryptography

- Cryptography emerged from the shadows to become an academic subject in the 1970s.
- Number of important developments in 70s:
  - development of DES (public) standard block cipher;
  - invention of public key cryptography, RSA and Diffie-Hellman key agreement;
  - start of public discussion of design and analysis of ciphers, including stream ciphers.

DES

- DES arose as a result of a competition by NBS in the US for a block cipher.
- This has become a model for development of new international crypto standards
- NIST (successor to NBS) has led two competitions giving us AES (DES successor) & SHA-3 (hash-function successor to SHA-1/2).
- Other bodies now launching similar competitions (e.g. recent competition for an authenticated encryption scheme).

Public key crypto and RSA

- Diffie and Hellman (at Stanford) wrote *New directions in cryptography* in 1976, describing:
  - notion of public key cryptography (PKC), and
  - the Diffie-Hellman (DH) key agreement method.
- This stimulated Rivest, Shamir and Adleman (at MIT) to develop the first practical public key encryption scheme, RSA.
- Interestingly, PKC, RSA and DH were independently developed in early 1970s by Ellis, Cocks and Williamson at GCHQ here in the UK.

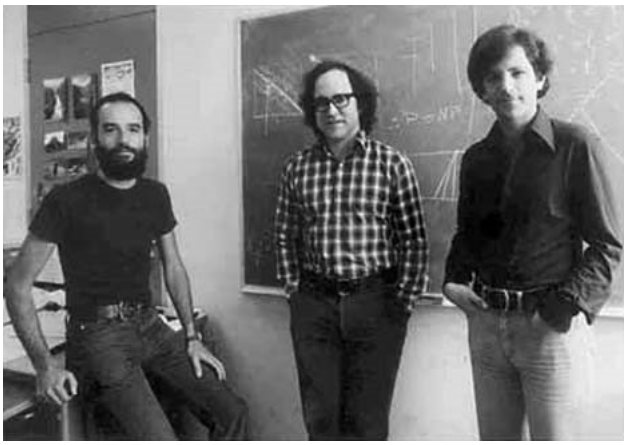
Merkle, Hellman and Diffie

7

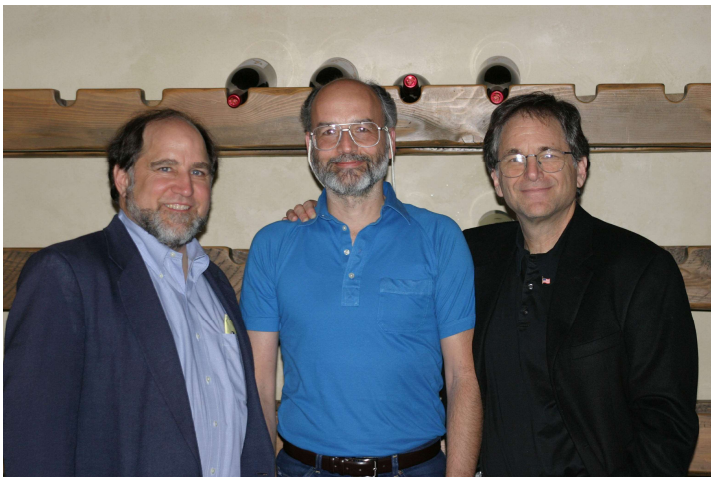
Diffie and Hellman

8

Shamir, Rivest & Adleman – then …



… and more recently (in the right order)



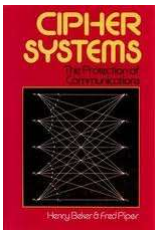
James Ellis, Clifford Cocks and Malcolm Williamson



Development of academic subject

- Three books published in the early 1980s played a major role in the development of academic crypto, by:
  - Alan Konheim (*Cryptography: A primer*),
  - Carl Mayer and Stephen Matyas (*Cryptography: A New Dimension in Computer Data Security*), and
  - Henry Beker and Fred Piper (*Cipher Systems*), here in the UK.

Beker and Piper: Cipher Systems



13

13

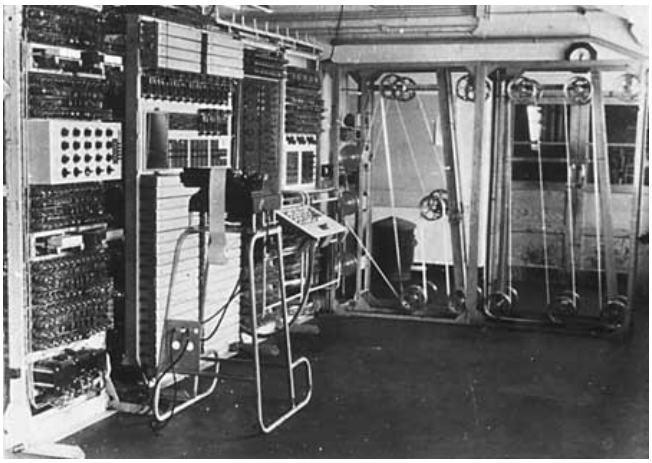
History of computing

- The development of computing as we know it today was presaged by the development of Colossus in the UK during the 2nd World War.
- Colossus, a fully programmable computer, was developed in 1943 to break the Lorenz SZ40/42 stream cipher.
- Alan Turing and Tommy Flowers played a major role in its development.

14

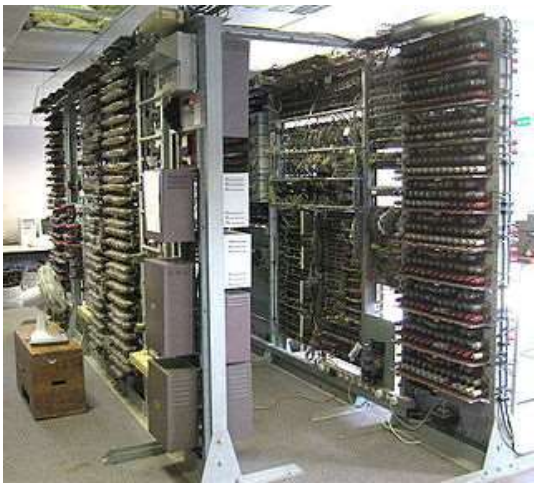
14

Colossus



15

Colossus rebuilt (at Bletchley)



16

Cryptography today

- Cryptography has gone from:
  - being something barely discussed in the public domain (pre-1970s), to
  - a technology all-pervasive in everyday life.

Agenda

1. Crypto – a (very) selective history
2. Crypto – its role in cyber
3. Challenges
4. The future

Real world crypto

- 'Early adopters' of cryptography were:
  - the banks (in the 1980s DES rapidly became a de facto international standard),
  - mobile telecommunications.
- For example, crypto has been widely deployed to protect PINs transferred between ATMs and banks for decades.
- Similarly, from the beginning in 1991, GSM SIMs incorporated secret keys and provided crypto-based authentication.

19

19

Pervasiveness of crypto

- Today, crypto is being used in almost every activity when using a phone, tablet, PC or Internet service.
- Examples include:
  - TLS almost universally used for browser-server interactions;
  - Transparent full disk encryption and many other crypto services in modern OSs;
  - Crypto-enabled proofs of identity including passports, identity tokens, etc.;
  - Digitally signed software updates for many types of device; …

20

20

Reliance on crypto

- The security of almost everything we do in the cyber world is dependent on cryptography.
- If poor choices are made regarding algorithm selection, protocol design, API design, or implementation, then a system can be made completely insecure.
- Getting it right isn't always easy (although there are many standards and guidelines).

Agenda

1. Crypto – a (very) selective history
2. Crypto – its role in cyber
3. Challenges
4. The future

Legacy issues – a case study: DES

- Because DES was the only obvious options back in the 1970s/80s, it was very widely adopted in commercial systems.
- System architectures were built around its 64-bit block length.
- This made switching to triple DES (to mitigate DES's short key length) relatively simple, as the block length is the same, and there is even a 'backwards compatible' option.

Alternatives to DES

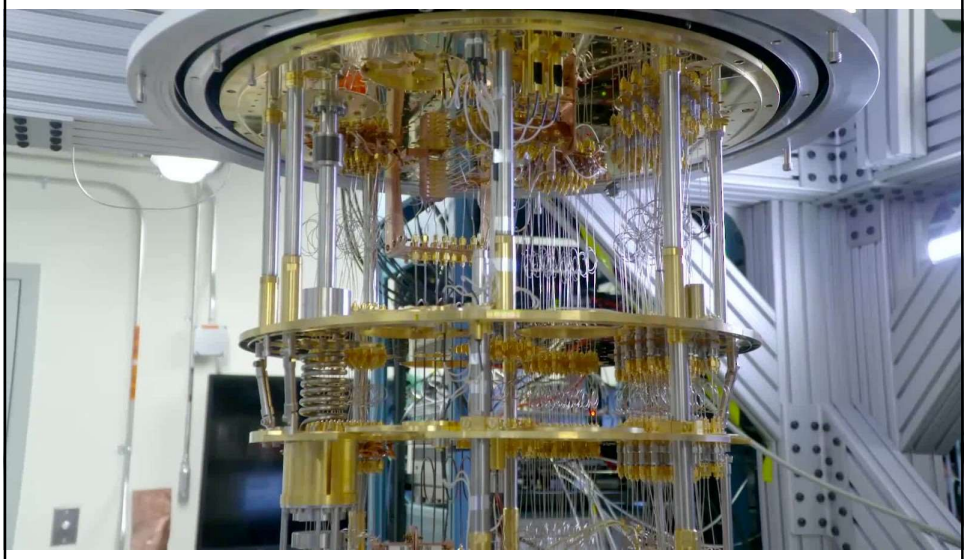
- We have had a good alternative for DES since 2002 – the *Advanced Encryption Standard* (AES) allows for long keys, e.g. of 256 bits and is believed to be secure.
- While it is incorporated in new systems, triple DES (and even single DES) has remained in very wide use.
- This is because of legacy systems, and the difficulty (cost and complexity) in replacing a cipher.

What does this mean?

- Triple DES will likely stay in use for years to come, despite its relative weakness.
- Sometimes it is simply impossible to replace it without completely redesigning a system.
- This suggests that we have major problems round the corner …

Quantum computers

- In recent years there has been much discussion of the impact of quantum computing on cryptography.
- There is no general agreement that large-scale, general purpose, quantum computers will ever be built – see, for example, Dyakonov's March 2019 IEEE Spectrum article – but huge efforts and gradual advances continue.
- Should such computers ever become available, they will have a major impact on the security of today's cryptography.



Potential impact

- If and when they arrive, we cannot be sure of the precise performance in terms of:
  - number of quantum operations per second;
  - number of quantum bits available.
- However, we can estimate the complexity of certain computations in terms of the number of quantum logic gates.
- From crypto perspective, there are two key algorithms that have been devised to run on quantum computers.

Shor's algorithm (1994)

- Greatly simplifies solving two problems, the hardness of which underlies all currently used asymmetric crypto:
  - factorising large integers;
  - computing discrete logarithms in elliptic curve or finite field multiplicative groups.
- Means that all currently used asymmetric algorithms are compromised for feasible key lengths.

29

29

Grover's algorithm (1997)

- Suppose function f has $|\text{Domain}(f)|=2^k$.
- Reduces complexity of searching for solutions x to $\boldsymbol{f(x)=y}$**, for known** $\boldsymbol{y}$, from 2^k function evaluations to $O(2^{k/2})$ function evaluations.
- A brute force key search (with known plaintext) involves solving such an equation.
- This effectively reduces key length for symmetric algorithms by half.
- Actually not so simple since function evaluation for AES involves lots of quantum computation.

30

30

Impacts

- For message authentication and digital signature applications a *just in time* approach is good enough.
- For applications involving encryption, or key establishment for encryption (e.g. TLS), an *as soon as possible* approach is warranted.

Replacing today's crypto

- For symmetric crypto, moving from 128-bit keys to 256-bit keys is more than adequate.
- For asymmetric crypto need new algorithms.
- Fortunately, NIST, ETSI, ISO/IEC and other standards bodies are working on it …
- The NIST *Post-Quantum Cryptography Standardization* competition is moving ahead – Round 3 candidates announced in July 2020.

General observations

- For every major application of cryptography a careful review of the impact of quantum computing needs to be done without delay.
- Such reviews should assess which parts of the system are vulnerable to quantum computing, and what the impact would be if these parts of the system are broken.

Reviews needed

- Reviews should consider how long it will take:
  - to replace crypto used in each part of the system;
  - to update the specifications;
  - to produce replacement implementations; and
  - to replace all existing deployed implementations.
- The total time could be very considerable, e.g., credit and debit cards have a typical lifetime of three-five years, so replacing all such cards could take a decade or more (and this doesn't even consider the time required to replace the supporting infrastructure).

Legacy

- The fact that we have struggled to replace triple DES suggests that moving to 'quantum safe' cryptography is going to be very difficult and costly.
- This is quite apart from the fact that we are still struggling to decide which public key ciphers we should use in a post-quantum world.

Agenda

1. Crypto – a (very) selective history
2. Crypto – its role in cyber
3. Challenges
4. The future

Some good news …

- Work has proceeded apace to develop a suite of asymmetric cryptosystems which appear to be secure.
- The NIST initiative is particularly important, but work is also going on elsewhere, e.g. in ETSI and ISO/IEC SC 27.
- Standardised security systems and protocols are increasingly being based on rigorous security analysis.

37

37

However, no time to relax …

- Problems are still being found, particularly in:
  - complex protocols using crypto, where attacks continue to be discovered years after adoption and use, e.g.:
    - long and tangled history of SSL/TLS, leading to TLS 1.3;
    - major security problems with other widely used protocols, including ssh and standardised messaging protocols;
  - crypto/system implementations, e.g. where:
    - carefully-designed specifications are not correctly followed;
    - a broad range of side-channel attacks have been discovered in widely used implementations;
    - random number generators, e.g. used for key selection, are not robust;
    - version-downgrade attacks are possible (because of legacy support).

38

38