Where are these things used

(Peeter's view)

The constructions we have seen

- Block ciphers
  - Differential cryptanalysis
- Stream ciphers — LFSRs
- Symmetric and asymmetric encryption
- Diffie-Hellman key agreement
- Signatures, message authentication codes
- Compression and hash functions
- Identification schemes
- Hard problems:
  - Factoring, RSA, quadratic residuosity
  - Discrete logarithms, Diffie-Hellman in (subgroups of)
    - $\mathbb{Z}_p^*$
    - Elliptic curves over finite fields

DES

- Proposed in 1975, standardized 1976
- Intended for sensitive, but *unclassified* government data
- Spurred an interest in cryptography outside certain agencies
- Short keys, short block length
- Hardware-oriented
- First large-scale application: securing the connections between banks and ATMs
  - DES$(k_{\text{secret}}, \cdot)$ also used as a random function

Block ciphers in 1990s

- FEAL
  - First variant proposed in 1987 by researchers at NTT
  - 64-bit blocks, 64-bit (later more) keys
  - Feistel network, byte-oriented design
  - Broken; was instrumental in the development of differential and linear cryptanalysis
- Idea (International Data Encryption Algorithm)
  - Proposed in 1991 by researchers at ETH Zürich
  - 64-bit blocks, 128-bit keys
  - Interesting mix of 16-bit operations
  - Patented in USA, Japan, some European countries (until 2011)
  - Included in PGP (and in Cybernetica's VPN product)
  - Together with Pentium MMX, inspired Helger to work on fast implementations of block ciphers

Block ciphers in 1990s

- BlowFish
  - Proposed by Bruce Schneier in 1993
  - 64-bit blocks, variable-length keys
  - Included (as an option) in lots of products http://www.schneier.com/blowfish-products.html
  - Was not so well-known in Estonia (?)
- RC5 ("Rivest's Cipher 5")
  - Proposed in 1994
  - Patented
  - Subject of the *RSA Secret-Key challenge*

Strengthened versions of DES

- Triple-DES
  - 168-bit keys ("112-bit strength"), 64-bit blocks
  - Either EEE- or EDE-mode
    - EDE-mode is backwards compatible with DES
  - Slow, but was ubiquitous, thanks to relationship with DES
- DESX
  - Proposed by Kilian and Rogaway in 1996
  - $\mathsf{DESX}_{k,k_1,k_2}(m) = k_2 \oplus \mathsf{DES}_k(m \oplus k_1)$.
  - Effective key length ≈ 119 bits.

US Export restrictions

- Dual-use technology — applicable both in commercial and in military sector.
- Exporting militarily useful technology from USA requires a license.
- The implementations of encryption algorithms were classified as munitions.
  - To export, one had to negotiate with the Dept. of Commerce.
  - Generally, the export versions of products were allowed to use up to 40-bit keys.
    - For example, Netscape had different versions. . .
- “Implemented in Europe” was a pretty strong selling point in 1990s.
- In late 1990s and 2000s, the rules have been relaxed. . .
- See also http://www.wassenaar.org

Competition for AES

- Submission: July 1998, AES chosen Oct. 2000
- Had to have 128-bit blocks, 128/192/256-bit keys
- 15 submissions, 5 picked to the second round
    - MARS, RC6, Rijndael, Serpent, TwoFish
- No obvious weaknesses known for any of them
- Hence speed was a big factor in making the final choice
    - Helger contributed
- These days, everybody uses AES as their block cipher. . .

Ciphers in GSM

- A5/1, A5/2. Were kept secret. Leaked in 1999.
  - A5/2 is a weakened version of A5/1
- A5/1: Three LFSR-s of 64 registers in total. Combined with XOR.
  - Irregularly clocked (the only non-linear part)
- 64-bit key, used as (sort of) the initial content of registers.
  - In fielded implementations, 10 bits are fixed.
- Weaknesses: short key, small internal state.
- A5/2 is extremely weak, and no longer used.

WEP / WPA

- WEP = Wired Equivalent Privacy
- RC4 (a stream cipher) + CRC32
  - When using RC4, certain details have to be taken into account. WEP does not do it.
  - CRC is not a MAC
- WPA = Wi-Fi Protected access
  - Uses RC4 (WPA2 uses AES in Counter mode)
  - A proprietary MAC (WPA2 uses CBC-MAC with AES)
- RC4 $\equiv$ Rivest's Cipher 4
  - A stream cipher that is not based on LFSRs
  - Internal state: a permutation of $\{0, 1, \ldots, 255\}$.
  - Intially, it is shuffled based on the key.
  - At each step, it is shuffled, and a byte is output.

Hash functions

- Construction:
  - Specify a compression function
    - ad-hoc design
  - Specify the padding
    - Add the length, pad to block size
  - Use Merkle-Damgård construction to get a hash function
- Used in signing, protocols, general integrity protection.
- SHA-1 still the most popular

Hash trees

- Physics: arrow of time $\equiv$ increase of entropy
- Crypto: arrow of time $\equiv$ application of one-way functions
  - If $y = h(z_1 \| x \| z_2)$ then "x existed before y"
    - But z_1, z_2 must be known
  - Take the "transitive closure" of the previous relation
- Hash trees are used to give short proofs of temporal order
  - Used in time-stamping

Message authentication codes

- Used to implement secure channels
- HMAC — probably the most popular construction
  - $\text{MAC}_{k_1,k_2}(m) = h(k_1 \| h(k_2 \| m))$
  - Actually, k_1 and k_2 are derived from the same key k
- SHA-1 is still the most popular hash function. . .

- A different use: a lightweight method to keep untrusted storage from modifying your files.
- In the EMV protocol, the card will compute a MAC for the transaction data using a key that it shares with the bank.
  - Default algorithm: CBC-MAC with DES

RSA encryption

- Was patented in USA and promoted by RSA corporation
- Patents expired at around 2000
- Used to encrypt symmetric keys in secure e-mail applications. . .
- But OpenPGP message format (RFC 4880) specifies ElGamal as the must-implement encryption
  - OpenSSL does not contain ElGamal
- Some key-exchange protocols also use public-key encryption to send a secret key from one party to another

Diffie-Hellman key exchange

- The first asymmetric primitive (1976)
  - ElGamal encryption proposed in 1984
- Used to agree on session keys
  - By, e.g., SSH
- Elliptic curves also used

Signatures

- Used in certificates (PKI)
- Also used to ensure the integrity of messages in DH key exchange
  - SSH uses DSA (must implement) or RSA
  - Both RSA and DSA have well-defined standards of implementation
- Used to sign documents
  - See, for example, http://digidoc.ee

Identification and Zero-knowledge

- General schemes are of theoretical interest only
- There exist efficient zero-knowledge protocols for certain tasks, but I am not aware of any widespread usage
  - In a more controlled environment, non-zero-knowledge methods can be attractive, too
  - E.g. passwords, or signatures to meaningless messages
- E.g. the identification done by Estonian ID-cards really means participation in SSL key exchange