COMP 424

Lecture 04
Advanced Encryption Techniques
(DES, AES, RSA)

Secret Key Systems

- A message M, encrypted with key K is denoted as $[M]^K$.
- Decryption is done with the same key and denoted: $[[M]^K]^K = M$.
- The basic disadvantage to these systems is a problem of combinatorics.

Public Key Systems

- A message M, from A to B is encrypted with B's public key and decrypted with B's private key.
  - Anyone and everyone can know B's public key.
- The encrypted message is denoted: $[M]^{KBpub}$.
- The decryption is denoted: $[[M]^{KBpub}]^{KBpriv} = M$.
- What the advantages and disadvantages?

Can Provide Authentication

- Reverse the use of the keys (encrypt with private and decrypt with public) and you can now authenticate who sent the message.
- $[[M]^{KBpriv}]^{KBpub} = M$
  - If B is the only person who holds the key Kbpriv then only B could have been the person to have encrypted M.

Increasing Confiedentiality

- A message from A to B could be encrypted as: $[[M]^{KApriv}]^{KBpub} = M$
- Decryption: $[[M]^{KBpriv}]^{KApub} = M$
- Where: $[[[[M]^{KApriv}]^{KBpub}]^{KBpriv}]^{KApub} = M$
- Wouldn't such a system be neat...
- (Not all asymmetric key cryptosystems have the propery: $[[M]^{KBpriv}]^{KBpub} = M$

Rivest-Shamir-Adelman (MIT 1977)

- Based on mathematical number theory.
- Relies on the underlying Number Theory of difficulty of determining multiplicative factors (prime numbers).
- Large numbers are extremely difficult to factor.
- Will this always be true? (probably not)
  - Moore's law (possibly)
  - Quantum / non-deterministic computing (probably)

RSA Basic property

- Given two (related) keys, *e* and *d* the basics of the RSA cryptosystem is:
  - P = E(*e*, D(*d*, P)) = D(*d*, E(*e*, P))
- That is to say that if we encrypt with *e* we can decrypt with *d* and if we encrypt with *d* we can decrypt with *e*.
- Math: $P^e \bmod n$ and $(P^e)^d \bmod n = P$
- Because the exponentiation of P is performed mod n it is difficult to factor n to recover plaintext

RSA details

- Select two large prime numbers p and q about 100 digits in length
- Compute $n = pq$ and $psi=(p-1)(q-1)$
- Choose an integer E between 3 and psi which has no common factors with psi
- Select an integer D, such that DE differs by 1 by a multiple of psi
- Make E and n public but keep p, q, D and psi private.

Some Problems

- Compromised keys can be used for masquerading and disclosure attacks
- Key distribution can be complex
- Not scalable in large systems
- Many secret (symmetric) key systems are weak compared to PKI (Public Key Infrastructure) approaches.

DES Overview

- Early 1970s (1972 died, 1974, 1976 adopted)
- Targeted for public cryptography
- Efficient and unbreakable
- Easy to understand
- Publishable
- Availability
- Economical
- Exportable

DES (IBM's lucifer)

- Combination of
  - Substitution
  - Transposition
- 16 cycles of each
- Processes plain text in blocks of 64 bits (56data bits plus 8 checking bits)
- Uses only standard arithmetic and logic
  - (RSA uses 500 and 1000 bit arithmetic operations.)

Unbreakable??

- Since 1976 (biven Moore's law) computers have increased in speed 2^{18} fold. (262,144 times)
- DES 56-bit is no longer considered secure.
- Solutions?
  - Use keys longer than 56bits?
  - Well... no. The DES algorithm is fixed at 56 bits. The nature of the algorithm requires it.

Double DES

- Use two keys k1 and k2 and perform the encryption $E(k_2,E(k_1,P))$
- Should be doubly strong just as two locks are harder to pick than one right?
- Wrong. Because of the nature of the DES algorithm the work required to crack the encryption increases from 2^{56} to just 2^{57}.
- Not worth the effort.

Triple DES (3DES)

- A simple trick solves the problem...
- $C = E(k_1,D(k_2,E(k_1,P)))$

Differential Cryptanalysis

- Biham and Shamir, 1990
- A method that investigates the change in cryptographic strength when a change is made to the encryption algorithm
  - Almost any change made to the DES algorithm weakens it.
  - Is DES optimal then? Possibly but the point is moot...

Breaking DES

- 1997: 3,500 machines where used to infer a DES key. It required four months to do so.
- 1998: special hardware (DES cracker) was construced at a cost of $100,000 and could find a DES key in just four days.
- So its still rather secure because the resources to break it are still rather expensive. But it is certainly on the verge of being obsolete.
- 3DES is still pretty good. 2^{112} bits effectively.

Future...

- AES: Rijndael