Tutorial 3

Aim

To illustrate basic cryptographic methods, and the effort needed to break them.

Questions

1. Given the ciphertext **ZLJBYPAF,** find the plaintext and the key. The cipher is a simple substitution of the shift-by-*n* variety.

2. Suppose that we have a computer that can test 2^{41} keys each second.
   (a) What is the expected time (in years) to find an 88 bit long key by brute force?
   (b) What is the expected time (in years) to find a 112 bit long key by brute force?
   (c) What is the expected time (in years) to find a 256 bit long key by brute force?

   Help

   To find the powers of two you can use a table such as at http://www.tsm-resources.com/alists/pow2.html.

3. A simple transposition cipher has the following ciphertext: ICBKAOREMDERAEA
   (a) What is the plaintext?
   (b) What would be the ciphertext, if you swapped columns 1 and 3 in the conversion table?

4. With public key encryption, A wants to send a message to B. Let A_{pub} and A_{priv} be A's public and private key respectively; similarly B_{pub} and B_{priv} for B. Suppose C knows both public keys but neither of the private keys.
   (a) If A sends a message to B, which key should it use so that only B can decrypt the message? (This is called secrecy)
   (b) Can A encrypt a message so that everyone can decrypt the message and they will know it came from A? (This is authenticity)
   (c) Can A achieve both secrecy and authenticity for a message? If yes how, if not why not?