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.

   Security
   n=7

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?

   2^{47} seconds ~ 4.462×10^{6} years

   (b) What is the expected time (in years) to find a 112 bit long key by brute force?

   2^{71} seconds ~ 74.872×10^{12} years

   (c) What is the expected time (in years) to find a 256 bit long key by brute force?

   2^{215} seconds ~ 1.67×10^{57} years

   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?

   I AM A CODEBREAKER

   (b) What would be the ciphertext, if you swapped columns 1 and 3 in the ciphertext?

   BCIKROAEEDMRAEAA

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.

   In asymmetric encryption, the keys cannot be calculated from each other in reasonable time. The public key can be made known to everyone wanting to communicate. The private key is kept secret. When a message is encrypted by the private key, the message can not be falsified. When a message is encrypted by the public key, the message can not be decoded by unauthorised parties. The applications of public-key cryptosystem include: digital signature (authentication), and information encryption/decryption. Common public-key algorithms include: RSA, EL Gamal (Deffie-Hellman algorithm is for key distribution).

   (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)

   The answer is key $\mathbf{B_{pub}}$, because B is the only one knowing key $\mathbf{B_{priv}}$. The information decrypted by $\mathbf{B_{priv}}$ must be encrypted by $\mathbf{B_{pub}}$.

   (b) Can A encrypt a message so that everyone can decrypt the message and they will know it came from A? (This is authenticity)

   Similarly, since the key $\mathbf{A_{pub}}$ is known publicly, and the information decrypted by $\mathbf{A_{pub}}$ must be encrypted by $\mathbf{A_{priv}}$, and A is the only one knowing key $\mathbf{A_{priv}}$, we can deduce that the message can only come from A (if the message is meaningful). Thus, the answer is the key $\mathbf{A_{priv}}$.

   (c) Can A achieve both secrecy and authenticity for a message? If yes how, if not why not?

   If Cyphertext = Encrypt(Encrypt(Plaintext, $\mathbf{A_{priv}}$), $\mathbf{B_{pub}}$), then both secrecy and authenticity can be achieved.
   We can discuss another case where Cyphertext = Encrypt(Encrypt(Plaintext, $\mathbf{B_{pub}}$), $\mathbf{A_{priv}}$). The attacker can easily obtain Encrypt(Plaintext, $\mathbf{B_{pub}}$) by decrypting the cyphertext with the key $\mathbf{A_{pub}}$. It is less secure in this case.