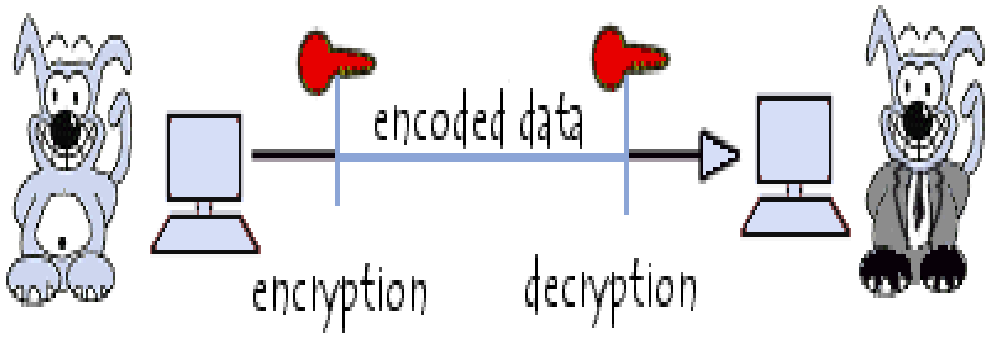
Private-key (or secret-key) cryptography

Symmetric encryption

Symmetric encryption (also called *private-key encryption* or *secret-key encryption*) involves using the same key for encryption and decryption.



Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

However, in the 1940s, *Claude Shannon* proved that to be completely secure, private-key systems need to use keys that are at least as long as the message to be encrypted. Moreover, symmetric encryption requires that a secure channel be used to exchange the key, which seriously diminishes the usefulness of this kind of encryption system.
The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of *N* people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to *N * (N-1) / 2*.
In the 1920s, Gilbert Vernam and Joseph Mauborgne developed the *One-Time Pad* method (sometimes called "One-Time Password" and abbreviated *OTP*), based on a randomly generated private key that is used only once and is then destroyed. During the same period, the Kremlin and the White House were connected by the famous **red telephone**, that is, a telephone where calls were

encrypted thanks to a private key according to the *one-time pad* method. The private key was exchanged thanks to the diplomatic bag (playing the role of secure channel).

Source: http://en.kioskea.net/contents/130-private-key-or-secret-key-cryptography