§3. The RSA Cryptosystem

The case of the Heptameron.

The RSA cryptosystem is a public-key cryptosystem used for secure data transmission. It is based on the difficulty of factoring large numbers and is named after its inventors, Ronald Rivest, Adi Shamir, and Leonard Adleman. The system is asymmetric, meaning that it uses a pair of keys: a public key for encryption and a private key for decryption. An encryption message can be sent using the public key, and only the corresponding private key can decrypt it.

We shall next discuss two particularly important examples of public key cryptosystems.

22. Problems of Encryption

Cryptographers (Wenceslas von Dornach and Drawing 1996). The two parties, Alice and Bob, exchange a pair of public keys over a secure channel. Alice encrypts a message using Bob's public key, and Bob decrypts it using his private key. This ensures that only Bob can read the message.

The most common problems for which public-key cryptosystems can be applied include

1. Authentication: verifying the identity of a user.
2. Confidentiality: protecting the content of a message.
3. Integrity: ensuring that a message has not been altered.
4. Non-repudiation: preventing a sender from denying the authenticity of a document or message.

24. Tests for Public Key Cryptosystems

In practice, the actual value of public key cryptosystems is significantly different, especially regarding performance.