MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Hybrid Encryption I

Author: Chair for Cryptology and IT Security
Ruhr-University Bochum

October 2010

Hybrid Encryption

A drawback of symmetric encryption schemes is the problem of key exchange. Prior to the actual encryption the parties have to exchange a secret key in a secure way. The encryption itself can be performed very efficiently.

Asymmetric encryption schemes solve the problem of key exchange by using a key pair consisting of public and private key. The data encryption, however, is very costly.

Hybrid Encryption

To use the advantages of both symmetric and asymmetric, in practise one often uses a hybrid encryption. This means that a random key K for some symmetric scheme is generated and the plaintext is encrypted using that scheme. To transfer this session key K to the receiver, a public key scheme is employed to encrypt the session key.

Challenge

- You eavesdropped on a hybrid encryption communication.
- You know that the asymmetric scheme RSA is used in its plain form, i.e. the session key is encrypted as $c = K^e \bmod N$.
- The session key itself is used in an 128 bit AES Cipher in ECB mode to encrypt the plaintext message.
- Find the plaintext message.

In the addidional file you will find the public RSA parameters (N,e) and the ciphertexts. The encryption of the session key under RSA is given as c_p and the encryption of the plaintext under AES using the session key is given as c_s.