Algorithm used:

AES – Symmetric Key Cryptography

RSA – Public Key Cryptography

Key Size:

AES Key size: 128 bits

RSA Key size: 2048 bits (.der format)

Algorithm Mode:

AES – Cipher Block Chaining (CBC) with ISO 10126 padding. CBC has XOR’ing process which hides plaintext patterns.

Using AES and RSA

On sender’s side

We take the plain text file and encrypt it with AES key.

We need to share the secret key with destination, so receiver can decrypt the file.

AES key cannot be sent in a plain way. So we use RSA to encrypt the AES key.

We use public key of the receiver to encrypt the AES key and private key of the sender to sign it.

On receiver’s side

We read the cipher file.

Verify the signature using the public key of the sender.

Decrypt it with private key and read the secret key i.e. AES key

Then we use this AES key to decrypt the encrypted message, and retrieve the plain text.