PKCS

Algorithm: Encryption using PKCS#1v1.5

Input : Recipient's RSA public key (n, e); k = |n| bytes; Data 'D' of length |D| bytes with |D| <= k-11

Output : Encrypted data block of length k bytes.

1. Form the k-byte padded message block EB
   EB = 00 || 02 || PS || 00 || D
   where || denotes concatenation and PS is a string of (k-|D|-3) non-zero randomly generated bytes(i.e., at least 8 random bytes)
2. Encrypt EB with the RSA Algorithm
   C = RSA(EB)
3. Output C

RSA Algorithm

Key Generation (at A)
Select two large primes p, q such that p is not equal to q
Compute n = p * q
Compute phi(n) = (p-1) * (q-1)
Select ‘e’ such that gcd (e, phi(n)) = 1
Compute d = e-1 mod phi(n)
A’s Public key is (e, n); A’s Private key is d

Encryption

Any party B wishing to send a message M to party A encrypts M using RSA as:

$$C = M^e \bmod n$$

Decryption

Party A decrypts ‘C’, received from party B, using his private key d as:

$$M = C^d \bmod n$$