RSA Encryption Algorithm

RSA algorithm is named after its inventors (Rivest, Shamir and Adleman). It is a pubic key cryptographic scheme. The public and private keys in this scheme are generated as follows:

Step1: Choose two large prime numbers "p" and "q" so that the product is equal to the integer "n", i.e., n = pq. The plaintext to be encrypted, say, "P" is represented as an integer less than "n." (This means "n" must be a large number)

Step2: Find a number "e" that is relatively prime to the produce (p-1)(q-1). Note that two numbers are said to be relatively prime if they have no common factors except 1. The public key is then given by {e,n}.

Step3: Find a number "d" such that the product de = 1 mod ((p-1)(q-1)). That is, "d" and "e" are multiplicative inverses of each other modulo (p-1)(q-1). The private key is then {d,n}.

Why does RSA work?
From the above steps we see that for any integer $P < n$, $P^{de} \pmod{n} = P \pmod{n}$.
RSA uses large binary keys, typically 512 bits long. It takes binary blocks of plaintext of length smaller than the key length and produces a ciphertext that is the same length of the key. If the integer "P" represents a block of plaintext then RSA encrypts "P" as follows:

Encryption: Ciphertext, $C = P^e \pmod{n}$

Note that the ciphertext, C is an integer between 0 and "n."
To decrypt, the following procedure is used:

Decryption: $C^d \pmod{n} = (P^e)^d \pmod{n} = P^{ed} \pmod{n} = P \pmod{n} = P$.

Example:

Suppose we want to encrypt the plaintext "RSA" using RSA encryption. Convert this to integers, "R" = 18 (its position in the English alphabet), "S" = 19, and "A" = 1. Let us choose p = 5 and q = 11. Then n = 55 and (p-1)(q-1) = 40. Let e = 7 (it is relatively prime to 40). Then, d = 23. Therefore, public key is {7,55} and private key is {23,55}.

Plaintexts, $P_1 = 18$, $P_2 = 19$, $P_3 = 1$ ("RSA"). Then,

$$C_1 = 18^7 \bmod 55 = 17;\ \ C_2 = 19^7 \bmod 55 = 24;\ C_1 = 1^7 \bmod 55 = 1$$

Therefore, the ciphertext is {17,24,1}.

Decryption: $17^{23} \bmod 55 = 18$; $24^{23} \bmod 55 = 19$; $1^{23} \bmod 55 = 1$

Note: To compute mod for large numbers, use this result:
$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$

Example:
$17^{23} \bmod 55 = 17^{16+4+2+1} \bmod 55 = ((17^{16} \bmod 55)(17^4 \bmod 55)(17^2 \bmod 55)(17 \bmod 55)) \bmod 55 = 18.$