RSA

RSA

- Select at random two large prime numbers p, q.
- Compute $n = pq$ and $\phi(n) = (p-1)(q-1)$.
- Select a small integer e such that $\gcd(e, \phi(n)) = 1$.
- Compute $d = e^{-1} \mod \phi(n)$.
- Publish the pair (n, e) as your RSA Public Key.
- Keep secret d, your RSA Private Key. Also keep $p, q, \phi(n)$ secret.

To encrypt a message M we find $C = M^e \mod n$.
To decrypt a cyphertext C we find $M = C^d \mod n$.

RSA Examples

- Perform encryption and decryption using the RSA algorithm, for the following:

1. p = 5; q = 11, e = 3; M = 9
2. p = 7; q = 11, e = 17; M = 8
3. p = 11; q = 13, e = 11; M = 7
4. p = 3; q = 11, e = 7; M = 5