

Handout: RSA Encryption

BACKGROUND STEP - Each entity creates a public and a private key:

1. Pick 2 "large" prime numbers p and q such that $p \neq q$
2. Let $m = (p-1)(q-1)$; let $n = pq$
3. Pick an integer e such that $1 < e < m$ such that e and m are relatively prime
4. Find the inverse of e modulo m (it is unique; call it d)
5. Your "public key" is the pair (n, e) . Make it public.
6. Your "private key" is the pair (n, d) . Keep it private!

TO SEND A MESSAGE:

1. Whatever message you have, encode it as a number in the agreed upon way. Suppose your message is the positive integer M .
2. Look up their public key; say it is (n, e) .
3. Make sure $M < n$
4. Send $M^e \bmod n$

TO DECODE A MESSAGE YOU ARE SENT:

1. Suppose your private key is (n, d) and you have received the message $C < n$
2. Find $C^d \bmod n$
3. Miraculously it will be M .