Math135 - November 9'th, 2015

Introduction To RSA Encryption

Cryptography

Cryptography is the practice and study of secure communications.

RSA

RSA is an effective public-key cryptosystem used to communicate private messages. In this class, we will prove why RSA works, and simulate encryption and decryption with small prime values.

Setting up RSA

1) Choose 2 large, distinct primes p and q.
2) Let $n = pq$.
3) Select an integer e so $gcd(e, (p-1)(q-1)) = 1$ and $1 < e < (p-1)(q-1)$.
4) Solve $ed \equiv 1 \pmod{(p-1)(q-1)}$.
5) Publish the public encryption key (e, n).
6) Keep secure the private decryption key (d, n).

Sending a Message

1) Look up the recipients public key (e, n).
2) Generate the message M so that $0 \leq M \leq n$.
3) Compute the ciphertext C as follows:
   $M^e \equiv C \pmod{n}$ where $0 \leq C \leq n$
4) Send C to the recipient.

Receiving/Decrypting a Message

1) Use private key (d, n).
2) Compute the message text R from C as follows:
   $C^d \equiv R \pmod{n}$ where $0 \leq R \leq n$
3) Hooray! You now have the plain-text message, R.