Introduction to RSA Cryptography

Arthur and Beatrice want to send private communications. They agree to encode their messages as numbers, and to then encrypt these before sending so that they won't be leaking information if the message is intercepted. They use the RSA Cryptosystem!

Setup

The intended receiver of the messages does the following.

1. Pick two prime numbers p, q and let $n := pq$.
2. Choose any $e \in \mathbb{Z}_{(p-1)(q-1)}$ with $\gcd(e, (p-1)(q-1)) = 1$.
3. Broadcast the pair (e, n), the *public key*.
4. Compute d, the inverse of $e \pmod{(p-1)(q-1)}$, the *private key* (kept secret).

Encryption

To encrypt a message $m \pmod{n}$, the sender computes $\widehat{m} = m^e \pmod{n}$; the sender sends $\widehat{m}$.

Decryption

To decrypt an encrypted message $\widehat{m}$, the receiver computes $m = \widehat{m}^d \pmod{n}$.

Examples

1. Let $p = 11$ and $q = 13$.
   (a) What are all possible public keys for this choice of p and q?
   (b) Encrypt message $m = 15$ to send to a receiver with public key $(17, 143)$.
   (c) Encrypt message $m = 15$ to send to a receiver with public key $(29, 143)$.
   (d) Encrypt message $m = 95$ to send to a receiver with public key $(29, 143)$.
   (e) Decrypt the message $\widehat{m} = 75$ sent to you if your public key is $(17, 143)$.
   (f) Decrypt the message $\widehat{m} = 75$ sent to you if your public key is $(29, 143)$.
   (g) Decrypt the message $\widehat{m} = 100$ sent to you if your public key is $(29, 143)$.
2. Arthur broadcasts public key $(25, 133)$ and Beatrice broadcasts the public key $(31, 143)$. They then send the following sequences of messages (where "A: (a, b, c)" means Arthur sends the messages a, b, and c in that order).
   (a) B: $(8, 23, 27, 1, 18, 20, 8, 14, 18)$
   (b) A: $(96, 37, 23, 27, 9, 85, 27, 4, 9, 85, 3, 73, 60, 97, 60, 27, 13, 1, 97, 96)$
   (c) B: $(48, 1, 20, 8, 27, 23, 19, 27, 59, 127, 127, 12)$
   (d) A: $(9, 27, 97, 96, 9, 14, 132, 27, 13, 1, 97, 96, 27, 9, 85, 27, 97, 96, 60, 27, 24, 60, 85, 97)$
   (e) B: $(127, 11, 1, 123, 27, 23, 27, 44, 23, 12, 12, 27, 19, 54, 54, 27, 123, 127, 14, 27, 20, 127, 48, 127, 18, 18, 127, 44)$
   (f) A: $(14, 9, 3, 60, 27, 97, 1, 12, 132, 9, 14, 84, 27, 97, 37, 27, 25, 37, 109)$

   What are Arthur and Beatrice saying? Explain why they are using a very bad encryption scheme (many reasons!).