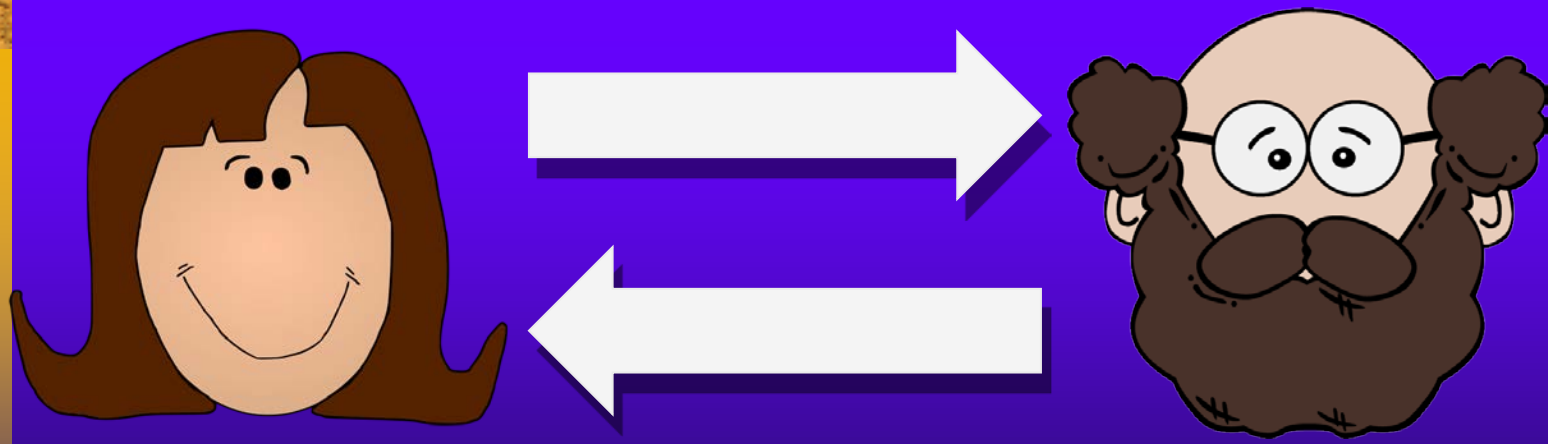
RSA Cryptography

The Alice and Bob Saga



The Dilemma

How can Alice ***securely*** send Bob a chest filled with awesome and amazing stuff?

1 Lock & 1 Key (Solution 1)

- Alice places a single padlock on the chest and sends a courier with the locked chest to Bob.

1 Lock & 1 Key (Solution 1)

- Issues:

Enter Diffie & Hellman (Solution 2)

- Alice places a lock on the chest and sends it to Bob.
- Bob adds his own lock to the chest and sends it back to Alice.
- Alice removes her lock and returns the chest to Bob
- Bob removes his lock and opens the chest.

Enter Diffie & Hellman (Solution 2)

- Issues:

Enter Rivest, Shamir, and Adelman (Solution 3)

- Bob sends Alice his padlock (opened).
- Alice places Bob’s padlock on the chest and sends the chest to Bob.
- Bob unlocks the chest using his key.

Enter Rivest, Shamir, and Adelman (Solution 3)

- Issues:

RSA Cipher in a Nutshell

1. The sender chooses two ***large*** prime numbers ***p*** and ***q***.
2. Compute $N = pq$.
   (*Note that* **N** *will be the modulus of the system and will be made public.)*
3. Compute $T = (p - 1)(q - 1)$.
   (*Note that* **T** *is Euler's totient function.)*
4. Choose public key ***e*** so that $3 < e < T$.
   (*Note that* ***e*** *must be an odd number and is typically prime.)*
5. Find the private key ***d*** so that $de \equiv 1 \bmod T$ which also implies that $de = 1 + bT$ for some integer ***b***.
   (Trial and error or the Extended Euclidean Algorithm may be used to find **d***.)*

RSA Cipher in a Nutshell

6. Encrypt the message.
   - Break the message up into appropriately sized blocks of letters and replace the letters with their representative number. Each number block ***must be*** smaller than **N.**
   - If you designate one of these number blocks as the number ***M*** and its encryption as the number ***C***, then $C = M^{(e)} \bmod N$.
   - A computer program or applet can help compute C. (i.e. https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html)
7. Decrypt the message.
   - $M = C^{(d)} \bmod N$.
   - Change the number back to the plaintext letters that they represent.

RSA Cipher Attacks

- Factor *N*
  - Trial Division
  - Pollard's p-1 Method
  - Pollard's *rho* Method
  - Elliptic Curve Method
  - Quadratic Sieve Method
  - Number Field Sieve Method

RSA Cipher Attacks

- Attack RSA Function
  - Low Private Exponent Attack
  - Partial Key Exposure Attack
  - Short Pad Attack

RSA Cipher Attacks

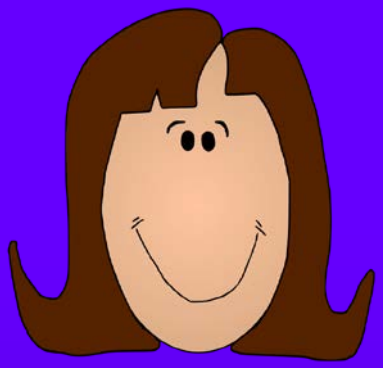
- Implementation Attacks
  - Timing Attacks
    (Estimating the time it takes to encrypt a message)
  - Power Analysis
    (Measuring the computer's power consumption)
  - Fault Analysis
    (Exploiting errors on key-dependent cryptographic operations)
  - Failure Analysis
    (Exploiting feedback decryption success/failure indications in implementation)

RSA Cipher
Interesting Facts & Applications

- Originally discovered in 1973 by British intelligence and classified as “top secret”.
- In 2009, a 768-bit product was successfully factored using the number field sieve (NFS). The process took over 2.5 years and used hundreds of computers. One single core 2.2 GHz AMD Opteron processor with 2 GB RAM would have taken 1500 years to complete the factorization alone.

RSA Cipher
Interesting Facts & Applications

- NIST recommends that modern cryptosystems use a minimum of 2048-bit keys until 2030 and 3072-bit key thereafter to be safe (see NIST Special Publication 800-57)
- RSA is used for internet encryption and authentication systems
  - digital signatures
  - secure ecommerce transactions
  - secure email
  - virtual private networks



That’s all folks…

Thanks for coming!

Sources

- Aoki, K., Franke, J., Lenstra, A. K., Thome, E., Bos, J. W., Gaudry, P, Kruppa, A., …, Zimmerman, P. (2010). *Factorization of a 768-bit RSA modulus*. Retrieved from http://eprint.iacr.org/2010/006.pdf

- Bar-Yosef, N. (2012). *Understanding public key cryptography and the history of RSA.* Retrieved from http://www.securityweek.com/understanding-public-key-cryptography-and-history-rsa

- Ohmart, P. (2011). *RSA encryption key size requirements* change in 2011. Retrieved from http://web.townsendsecurity.com/bid/23970/RSA-Encryption-Key-Size-Requirements-Change-in-2011