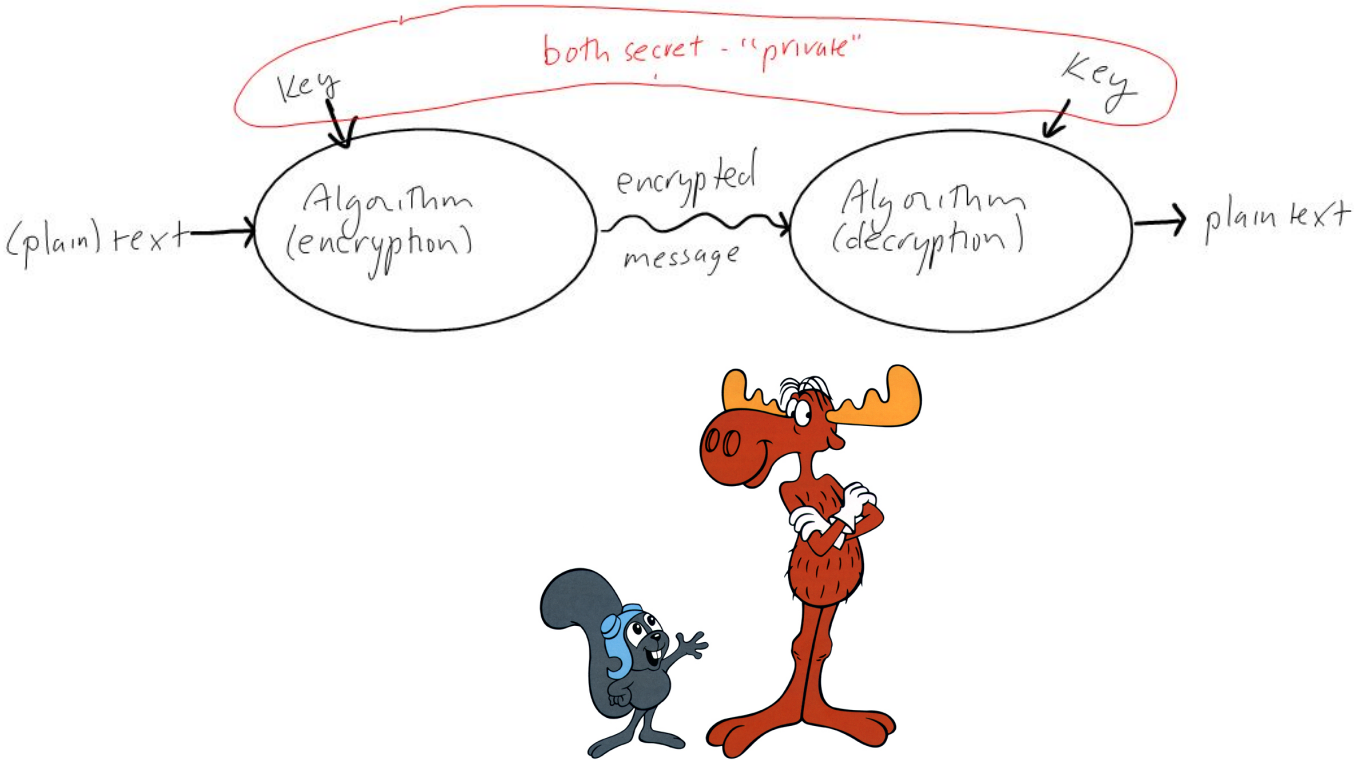
Public Key Cryptography - Math 100 Spring 2015

## 1 Cryptography

General Picture:



Features:

1. Rocky and Bullwinkle both know algorithm
2. Same information (key) is used for encryption/decryption, known to both Rocky and Bullwinkle
3. If key falls into Boris and Natasha's hands, they can decode any message
4. Therefore Rocky and Bullwinkle need to exchange their keys in a secure manner

Other issues:

1. There are many historical codes and ciphers, testaments to their inventors' cleverness.
2. Example: Substitution cipher
   EG: ROT13

   ABCDEFGHIJKLMNOPQRSTUVWXYZ ⇒
   NOPQRSTUVWXYZABCDEFGHIJKLM

   Math is fun! ⇒ Zngu vf sha!
3. Example: Transposition cipher

   EG: Rail Fence Cipher

   Math is fun! ⇒

   ```
   M*** ****f***
   *a*h*i* **u*!
   **t***s****n*
   ```

   ⇒ M fahi u!tsn
4. If encryption algorithm is simple enough, code-breaker can deduce the algorithm/key

5. Example: Enigma (cf *The Imitation Game*)

Plaintext typed one character at a time into electromechanical encoding device

Character is replaced by a substitution cipher

Each keystroke causes the device to change cipher according to mechanical workings (rotors, gears, etc.)

Decoding done with similar machine, assumes same starting point

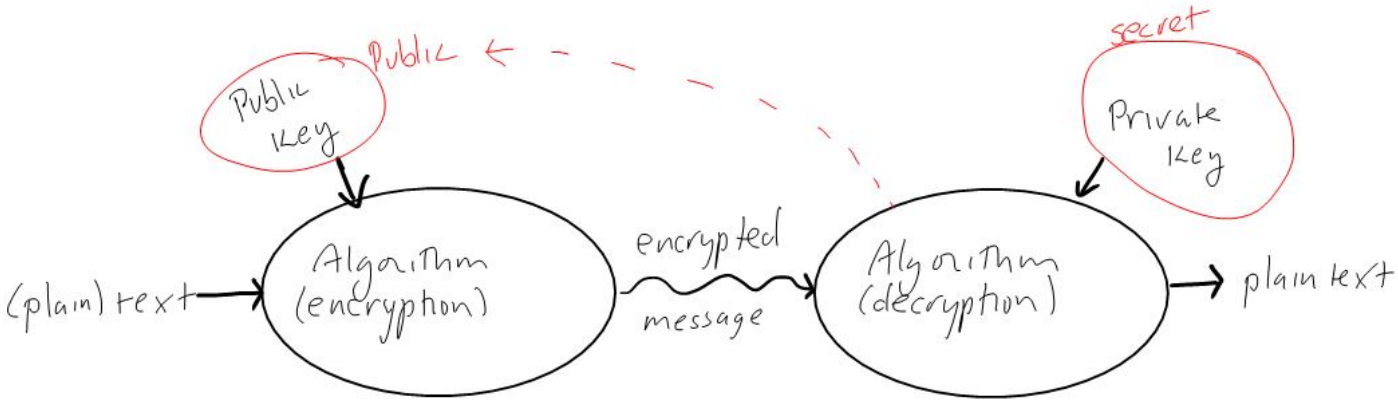
Difficulty in breaking depends on complexity of machine (number of rotors, etc)

Operation is covered by an area of math called Group Theory


(image from `https://commons.wikimedia.org/wiki/File:Enigmas.jpg`)

## 2 Public-key (RSA) cryptography

- Rivest, Shamir, Adleman 1977 (hence "RSA")
- (Possibly invented first by GCHQ mathematician Clifford Cocks in 1973)
- Versions of this now dominate cryptography for anything from high-security communication to secure web pages (https)



- Features:

1. Bullwinkle shares/publishes an *encryption key*, keeps *decryption key* secret
2. Rocky (or anyone!) uses encryption key to encrypt plain text
3. Bullwinkle uses decryption key to decrypt text
4. Bullwinkle doesn't need to share the decryption key with anyone, and it is almost impossible to figure out the private decryption key from the public encryption key
5. Encryption and decryption is based on arithmetic mod n (so is easy)
6. The cracking difficulty is based on the computational difficulty of factoring large numbers

## Operation

Setup:

1. Bullwinkle picks $p, q$ large primes so that $n = pq$(="modulus") is hard to factor, really big.
2. Bullwinkle picks $e$"public exponent", any number $< n$ relatively prime to $(p-1)(q-1)$
3. $d$ ="private exponent" is the unique solution to
$$ed \equiv 1 \mod (p-1)(q-1)$$
4. Bullwinkle publishes both $n$ and $e$ on his website

Encryption:

1. Rocky converts the text message to a (probably large) number $M$
2. Rocky encodes this to $C = M^e \mod n$
3. (Note: if $M > n$ then information will be lost! That's why $n$ should be big.)
4. Rocky sends $C$ to Bullwinkle.

Decryption:

1. Bullwinkle computes $C^d \mod n$
2. Mathematics says: result is $M$
3. Bullwinkle can convert $M$ back into text.

So what's left?

1. Given $e, p, q$, how do we find the unique $d$ such that $ed \equiv 1 \mod (p-1)(q-1)$

   More generally, given the equation $ax \equiv b \mod m$, how do we solve for $x$? Is it even always possible?

2. Show that the value Bullwinkle computes:

$$M = C^d \mod n$$

   really is the original message. (It isn't magic!)

So, let's recall:

$$p \text{ and } q \text{ are large primes}$$
$$n = pq$$
$$e < n$$
$$\text{GCF of } e \text{ and } (p-1)(q-1) \text{ is } 1$$
$$d \text{ (the private exponent) satisfies}$$
$$ed \equiv 1 \mod (p-1)(q-1)$$
$$M = \text{ the message } = \text{ an integer less than } n$$

Rocky computes

$$C = M^e \mod n$$

Bullwinkle computes

$$C^d \mod n$$

Is this last value back to $M$? Does

$$\begin{aligned} C^d \mod n &= (M^e)^d \mod n \\ &= M^{ed} \mod n \\ &\stackrel{?}{\equiv} M \mod n \end{aligned}$$

In other words, is $M^{ed} - M$ divisible by $n$?

Remember, $n = pq$. **PROOF BY CASES:**

**Case 1:** $p$ and $q$ both divide $M$. Then $n|M$, so $M \equiv 0 \equiv M^{ed} \mod n$.

**Case 2:** either $p$ or $q$ (but not both) divide $M$.

Suppose (for definiteness) that $q|M, p \nmid M$. Since

$$ed \equiv 1 \mod (p-1)(q-1),$$
$$ed = 1 + k(p-1)(q-1) \text{ for some } k.$$

So,

$$\begin{aligned} M^{ed} - M &= M(M^{ed-1} - 1) \\ &= M(M^{k(p-1)(q-1)} - 1) \\ &= M((M^{p-1})^{k(q-1)} - 1) \end{aligned}$$

We'd be done if we knew that $M^{p-1} \equiv 1 \mod p$, since then $q$ would divide the first term and $p$ the second, so $n = pq$ divides the product.

**Case 3:** neither $p$ nor $q$ divide $M$.

As in case 2, if we know that the conditions on $p$ and $q$ imply $M^{p-1} \equiv 1 \mod p$ and $M^{q-1} \equiv 1 \mod q$ then $p$ and $q$ would *both* divide $(M^{ed-1}-1)$, so $n|M^{ed} - M$.

To make these two cases work, we can invoke a thing called

**Fermat's Little Theorem** If $p$ is prime and $p \nmid a$ then $a^p \equiv a \mod p$,
equivalently $a^{p-1} \equiv 1 \mod p$

The proof (using necklaces!) will be done in class.