University of Colorado **Boulder**

Department of Computer Science
CSCI 2824: Discrete Structures
Chris Ketelsen

Cryptography

Simple Encryption Schemes

The Caesar Cipher

One of the earliest known cryptographic ciphers was used by Julius Caesar. His strategy was to simply shift each letter of the alphabet forward 3 places (wrapping around when you get to the end). In this scheme:

$$A \to D \qquad K \to N \qquad Y \to B$$

This is often called a **Caesar Cipher** or a **Shift Cipher**

Mathematically, we can accomplish this by assigning to each letter a number between 0 and 25

$$A \to 0 \qquad K \to 10 \qquad Y \to 24$$

The encoding can be done by passing the value through a shift function modulo 26, i.e. $F(M) = (M + 3) \mathbf{mod}\ 26$

The Caesar Cipher

In general, for a shift k we use the function

$$F(M) = (M + k) \textbf{ mod } 26$$

To encode a message

- Convert letters to numbers between 0 and 25
- Pass each value through $F(M)$

Example: Encode *HELLO WORLD* using shift $k = 5$

HELLO WORLD is 7 4 11 11 14 22 14 17 11 3

Shifting gives:

The encoded message is then ____________________

The Caesar Cipher

How do we decode a message like *MJQQT BTWQI* ?

If we know the shift then it's easy, we just run it through the inverse

$$F^{-1}(C) = (C - k) \textbf{ mod } 26$$

Why is this a very unsecure cipher?

The Affine Cipher

Instead of just shifting, multiply and then shift

$$F(M) = (aM + b) \ \mathbf{mod}\ 26$$

where a and b are integers and $\gcd(a, 26) = 1$

The Affine Cipher

Suppose we know a and b, how could we decode a message?

Suppose we have an encrypted character C which we know satisfies

$$C \equiv aM + b \pmod{26}$$

We need to solve this congruence for M. Subtract b from both sides

$$C - b \equiv aM \pmod{26}$$

To solve for M we need the modular inverse of a (which we know exists because $\gcd(a, 26) = 1$). Call this inverse $\bar{a}$, then

$$M \equiv \bar{a}(C - b) \pmod{26}$$

The Affine Cipher

Example: Use an affine cipher with $a = 7$ and $b = 13$ to encrypt the letter E

The numerical value of E is 4, so we have

$$E \to a \cdot 4 + b = 7 \cdot 4 + 13 = 41 \equiv 15 \pmod{26} \to P$$

The Affine Cipher

Example: Find a decryption formula for the affine cipher in the previous example and use it to decrypt the character *P*

We need to compute the inverse of 7 modulo 26

$$\begin{aligned} 26 &= 3 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

$$\text{Then after some algebra:} \quad 1 = 3 \cdot 26 - 11 \cdot 7$$

So the inverse of 7 modulo 26 is -11

The Affine Cipher

Example: Find a decryption formula for the affine cipher in the previous example and use it to decrypt the character *P*

So a decryption formula is given by

$$F^{-1}(C) = -11(C - 13) \textbf{ mod } 26$$

To decrypt *P* we then have

$$P \rightarrow -11(15 - 13) \textbf{ mod } 26 = -22 \textbf{ mod } 26 = 4 \rightarrow E$$

Private Key Encryption

We've now looked at two very simple cipher-schemes

Shift Encrypt: $C = F(\ M\ ) = (\ M + k\ )\ \mathbf{mod}\ 26$

Shift Decrypt: $M = F^{-1}(\ C\ ) = (\ C - k\ )\ \mathbf{mod}\ 26$

Affine Encrypt: $C = F(\ M\ ) = (\ aM + b\ )\ \mathbf{mod}\ 26$

Affine Decrypt: $M = F^{-1}(\ C\ ) = \bar{a}(\ C - b\ )\ \mathbf{mod}\ 26$

Both of these ciphers are examples of **Private Key Encryption**

Both sender and receiver have to know the keys (k or a and b)

Private Key Encryption

This is problematic on a large scale

Imagine that you're a bank trying to send secure messages to hundreds of thousands of customers. That's a lot of keys that have to somehow be decided upon and shared completely in secret.

The solution to this problem is **Public Key Encryption**

Public Key Encryption allows senders and receivers to determine secret keys by transferring public information completely in the open