August 31, 2017 Class Notes

Nikki Backert

Caesar Cipher

Encryption:

$$E(x) = x + \kappa \pmod 26, \qquad 0 <= k <= 25$$

Decryption:

$$D(X) = x - \kappa \pmod 26$$

Cryptanalysis

Kerchoff's Principle (1883)
Whenever you are analyzing the security of a cryptosystem, you should assume the enemy knows everything about the system except for the key being used.

Possible Attacks: Ciphertext only: Eve only has access to ciphertext of message - every modern cryptosystem protected against this Known plaintext attack: Eve has both plaintext and ciphertext of at least one message (she wants to determine the key) Chosen plaintext attack: Eve gets a copy of the encrption machine and can encrypt any plaintext she wants and observe the ciphertext (she wants to determine key) Chosen ciphertext attack: Least likely. Eve gets a copy of decryption machine, can decrypt any ciphertext she wants
Attack the Caesar cipher: Ciphertext only: frequency attack/analysis Brute force: try every possible key Known plaintext: Suppose we learn a plaintext "c" corresponds to the ciphertext "F"; we can determine key by shifting plaintext by 3 (c = 2, f = 5) $E(2) \equiv 5 \pmod{26}$ $2 + K = 5 \pmod{26}$ $K \equiv 3 \pmod{26}$ Chosen plaintext: Encrypt "a" and know that shift of encrypted letter is K(a) = 0 then the ciphertext is treated as a number is the key Chosen ciphertext: Choose "A" and shift backwards for key

Modular Arithmetic

We can work "modulo" any positive integer m. All arithmetic we do we take our answer and divide by m and take the remainder. For fixed m the only possible values are 0,1,2 ... m-1. $m \equiv 0 \equiv -m \pmod{m}$. *Fractions not allowed with modular arithmetic. Addition, subtraction, multiplication always allowed
Definition: The. number $a \pmod{m}$ has an inverse $b \pmod{m}$ if $ab = 1 \pmod{m}$. In this case we call a invertible $\pmod{m}$.

Ex: $m = 7$ $\alpha = 4$ Let $\beta = 2$, $\alpha * \beta = 4 * 2 = 8 \pmod 7 = 1 \pmod 7 \alpha^-1 = 2 (mod 7)$
Theorem: $\alpha \pmod m$ is invertible modulo m if and only if $\gcd(\alpha, m) = 1$.
Division is only allowed modulo m by invertible elements if $\gcd(\alpha, m) = 1$, then to divide by α, multiply by α^{-1}.

Affine Cipher

key $(\alpha, \beta) \pmod{26}$

$$E(x) = \alpha x + \beta \pmod{26}$$
$$D(Y) = Y = \alpha x + \beta \pmod{26}$$
$$Y - beta = \alpha x \pmod{26}$$

Since m is 26, to divide by α it cannot be 13 and it must be odd.

$$D(Y) = \alpha^{-1}(Y - \beta) \pmod{26}$$
$$Y - B = \alpha x \pmod{26}$$
$$\alpha^- 1(Y - B) = x \pmod{26}$$

Ex: $\alpha = 9$, $\beta = 3$ Encrypt: "hi" (h=7, i=8)

$$E(h) = \alpha x + \beta \pmod{26}$$

$$= 9 * 7 + 3 \pmod{26}$$
$$= 11 + 3 \pmod{26}$$
$$= 14 \pmod{26}$$
$$= "o"$$

$$E(i) = 9 * 8 + 3 \pmod{26}$$
$$= 72 + 3 \pmod{26} = 20 + 3 \pmod{26}$$
$$= 23 \pmod{26}$$
$$= "x"$$

$$"hi" = "OX"$$

How many keys are there for the affine cipher?
β has (0,1 ... 25) = 26 possibilities
α has (1,3,5,7,9,11,15,17,19,21,23,25) = 12 possibilities
Total number of keys = $26 * 12 = 312$ possibilities

Attacks on Affine Cipher: Ciphertext only: frequency analysis, brute force attack

Known plaintext: Need to know 2 different letters to figure out key. Suppose g = C, j = 9, z = 25 z = U

$$E(9) = 2 \pmod{26}$$

$$E(25) = 20 \pmod{26}$$

$\alpha 9 + \beta = 2 \pmod{26}$

$-\alpha 25 + \beta = 20 \pmod{26}$

$\alpha 16 = 18 \pmod{26} (1)$

Multiply equation (1) by the inverse of 16 to find α and then plug into equation(1) to find β.