August 29, 2018 Class Notes

Alexandra Emory

September 10, 2018

Cryptanalysis-The Study of how to analyze and break cryptosystems.
Kerchov's principle: Developed in 1800's when analyzing a cryptosystem one should assume the attacker, or"Eve" knows everything about the system except the key.
4 different attacks:

1. Cipher text only attack:
   Ever has a copy of the cipher text but nothing else.
   Goal: Determine the plain text or (even better) the key.

2. Known plain text attack:
   Eve knows a cipher text along with the corresponding plain text.
   Goal: Determine the key.

3. Chosen plain text attack:
   Ever has access to the encryption machine and can enc any message she wants and see the output.
   Goal: Recover the key.

4. Chosen cipher text attack:
   Eve had access to the decryption machine and can decrypt any message she wants.
   Goal: Recover the key.

Suppose: Ever wants to attack a Caeser cipher using each one of the attacks.

- Cypher text only attack:
  Eve can use brute force (only 26 possible keys) or use frequency analysis (see what letters are most frequent and work backwards)
- Known plain text attack:
  Now Eve can recover the key using just a single letter.
  ex. Suppose Eve learns that corresponds to the plain text "d".

"T"$->19$
"d"$->3$
$E(3) = 3 + k \equiv 19(mod26) -> k = 16(mod26)$

- Chosen plain text attack:
  Eve can pick the letter "a" and encrypt it.
  The result is $E(0) \equiv 0 + k(mod26)$ Eve recovers the key immediately.

- Chosen cipher text:
  Eve can pick the letter "a" again and the result would be -key
  $D(0) \equiv 0 - k(mod26)$ She negates the result to recover k.
  Note: $-2 = 24(mod26)$. If $k = 2$ and Eve decrypts "a"
  $\equiv 0 - 2 \equiv -2(mod26)$
  $k \equiv 24(mod26)$
  $k \equiv -24(mod26)$
  $\equiv 2(mod26)$

All the rules of regular arithmetic carry over to modular arithmetic.

- Addition
- Subtraction
- Multiplication
- (Sometimes) Division*

*not allowed to have fractions in modular arithmetic

The only way to divide is to multiple by a different modules that is the multiplicative inverse of the thing we want to divide.
Division (mod 26) is only only by numbers that have a multiplicative inverse

Fact: The number a (mod 26)has a multiplicative inverse $b(ab \equiv 1 mod m)$ if $gcd(a, m) \equiv 1$.

Affine Cipher:
$key : (\alpha, \beta)$
$E(x) = \alpha x + \beta(mod26)$
EX. Pick the key $\alpha = 3$ $\beta = 7$. Encrypt the letter "f". "f" -> 5
$E(5)3(5) + 7(mod26)$
$\equiv 15 + 7 \equiv 26) \equiv$ "V"
How can we recover the plain text? What is the decryption
$y \equiv \alpha x + \beta(mod26)$
Solve this for x (mod 26)
$y - \beta \equiv \alpha x(mod26)$
$\alpha^{-1}(y - \beta) \equiv x(mod26)$
$D(y) \equiv \alpha^{-1}(y - \beta)(mod26)$

What if $\alpha = 3$ and $\beta = 7$?
What is $3^{-1}(mod 26)$?
$3^{-1} = 9(mod 26)$
$D(y) \equiv 9(y-7)(mod 26)$
$\equiv 9y - 63(mod 26)$
$\equiv 9y + 15(mod 26)$
Note: $-63 \equiv -11(mod 26)$

()How did we know that $3^{-1} \equiv 26$?
$3 * 9 \equiv 27 \equiv 1(mod 26)$
(Right now just use the multiplicative table on the website)

Example: Decrypt "V" -> 22
$D(22) \equiv 9(22) + 15(mod 26)$
$\equiv 16 + 15(mod 26)$
$\equiv 31 \equiv 5(mod 26) - >$"f"

How many keys are there? How many choices are there for α, β?
We need α to have a multiplicative inverse.
We need a α with $gcd(\alpha, 26) = 1$ so α can't be even or 13.
so α can be $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$ - 12 possibilities.
26 possibilities for β
$12 * 26 \equiv 312$ total possibilities ($\alpha = 1$ $\beta = 0$ is boring though).

Attack the Affine Cipher:
Cipher Text only attack:
Brute force all 312 possibilities or do a frequency analysis.

Known plain text attack:
Suppose "Eve" learns that "k" encrypts to "Y" and "h" encrypts to "F".
"k" -> 10 "h" -> 7
"Y" -> 24 "F"-> 5
$\alpha(10) + \beta \equiv 24(mod 26)$
$-\ \alpha(7) + \beta \equiv 5(mod 26)$
$- - - - - - - - - - - - - - -$
$(9)\alpha(3) + 0 \equiv 19(9)(mod 26)$
$\alpha(3) * 9 \equiv 19 * 9$
$\alpha \equiv 15$ Plug in α for β
$\alpha(7) + \beta = 5(mod 26)$
$=> 15(7) + \beta = 5(mod 26)$
$1 + \beta = 5(mod 26)$
$\beta = 4$
Key: $(15, 4)$

Chosen plain text attack:
Eve encrypts "a".

$E(0) \equiv \alpha(0) + \beta \equiv \beta(mod 26)$
Now she encrypts "b".
$E(1) \equiv \alpha + \beta(mod 26)$ subtract β to recover α.