Section 1.1: Some Simple Cryptosystems Part 1

Math 495, Fall 2008

Hope College

August 27, 2008

Elements of a Cryptosystem

- $\mathcal{P} =$ the set of possible plaintexts
- $\mathcal{C} =$ the set of possible ciphertexts
- $\mathcal{K} =$ the keyspace (the set of possible keys)
- For eack $K \in \mathcal{K}$, there is an encryption function $e_K : \mathcal{P} \to \mathcal{C}$ and a decryption function $d_K : \mathcal{C} \to \mathcal{P}$ satisfying $d_K(e_K(x)) = x$ for all $x \in \mathcal{P}$.
- Note that, for all $K \in \mathcal{K}$, e_K must be an injective function, i.e.

$$x_1 \neq x_2 \;\Rightarrow\; e_K(x_1) \neq e_K(x_2).$$

Modular Arithmetic

- Let m be a positive integer. Given integers a and b, we say $a \equiv b \pmod{m}$ if $b - a$ is divisible by m.
- Every integer a is equivalent $\pmod{m}$ to precisely one element r of $\{0, 1, \ldots, m-1\}$, and we refer to this element r as $a \bmod m$.
- We set $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, and we note that addition and multiplication can be defined as operations on $\mathbb{Z}_m$.
- For example, working in $\mathbb{Z}_{26}$ we have

$$14 + 20 = 34 \equiv 8 \pmod{26},$$

and

$$5 \cdot 7 = 35 \equiv 9 \pmod{26}.$$

Therefore, in $\mathbb{Z}_{26}$, $14 + 20 = 8$ and $5 \cdot 7 = 9$.

- Under these operations, $\mathbb{Z}_m$ satisfies the properties required to be an Abelian group (and, in fact, a commutative ring).

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$ (or $\mathbb{Z}_m$)
- For all $K \in \mathbb{Z}_{26}$ and $x \in \mathcal{P}$, define

$$\begin{aligned} e_K(x) &= x + K \pmod{26} \\ d_K(x) &= x - K \pmod{26} \end{aligned}$$

- We use the following text-to-numeric conversion:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Suppose $K = 7$. The plaintext 'ihavefoundthekey' will yield

x	8	7	0	21	4	5	14	20	13	3	19	7	4	10	4	24
$e_K(x)$	15	14	7	2	11	12	21	1	20	10	0	14	11	17	11	5

which yields the ciphertext 'POHCLMVBUKAOLRLF'.

Cryptanalysis

- Cryptanalysis attempts to answer the question, “If Oscar is allowed to see the ciphertext, can he use this information to discover the plaintext?”
- For the shift cipher on $\mathbb{Z}_{26}$, there are only 26 possible keys, and therefore the decryption key can be found quickly using an exhaustive key search. For this reason, the number of possible keys (i.e. the cardinality of the keyspace $\mathcal{K}$) becomes an important factor in constructing secure cryptosystems.

Substitution Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$
- $\mathcal{K} =$ the set of all permutations of $\{0, 1, \ldots, 25\}$.
- $K \in \mathcal{K}$ is chosen at random and used as the encryption function.
- For example,

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
L	T	Y	G	N	A	O	Q	B	W	Z	X	D	S	I	U	E	P	H	M	C	J	V	R	F	K

- There are $26! \approx 4.03 \times 10^{26}$ possible keys, making an exhaustive key search infeasible.

Affine Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$
- $\mathcal{K} =$ certain pairs $(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$.
- $e_K(x) = ax + b \mod 26$.
- For what pairs (a, b) is this function $e_K(x)$ injective?
- **Theorem:** Let $a, b \in \mathbb{Z}_{26}$. The following are equivalent:
  - The function $e_K(x) = ax + b \mod 26$ is injective.
  - The element $a \in \mathbb{Z}_{26}$ has a multiplicative inverse.
  - The greatest common divisor of a and 26 is 1 (i.e. a is relatively prime to 26).
- The elements $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ of $\mathbb{Z}_{26}$ are relatively prime to 26. Therefore, there are $12 \cdot 26 = 312$ possible keys for an affine cryptosystem on $\mathbb{Z}_{26}$.

Example of an Affine Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ with $K = (5, 8)$.
- The plaintext 'danger' yields

x	3	0	13	6	4	17
$e_K(x)$	23	8	21	12	2	15

  which leads to the ciphertext 'XIVMCP'.
- Since the encryption function is $y = 5x + 8$, the decryption function can be written as $x = 5^{-1}(y - 8)$, where 5^{-1} represents the multiplicative inverse of 5 mod 26.
- An exhaustive search shows that $5^{-1} = 21$, and therefore $d_K(y) = 21(y - 8)$.