Section 1.1: Some Simple Cryptosystems Part 2

Math 495, Fall 2008

Hope College

September 1, 2008

Vigenère Cipher

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$
- The plaintext is arranged into 'vectors' of length m, and then the chosen vector K is added to each vector.
- With $m = 5$ and $K = (17, 7, 5, 10, 11)$, the plaintext 'ihavefoundtheproblem' will produce

x	8	7	0	21	4	5	14	20	13	3	19	7	4	15	17	14	1	11	4	12
+	17	7	5	10	11	17	7	5	10	11	17	7	5	10	11	17	7	5	10	11
$e_K(x)$	25	14	5	5	15	22	21	25	23	14	10	14	9	25	2	5	8	16	14	23

which yields the ciphertext 'ZOFFPWVZXOKOJZCFIQOX'.

Hill (Matrix Block) Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, and $\mathcal{K}$ is the set of $m \times m$ invertible matrices with entries in $\mathbb{Z}_{26}$.
- The plaintext is arranged into 'vectors' or 'blocks' of length m. For a chosen key matrix K, each block is encrypted using a matrix product $y = xK$ (computing mod 26).
- For example, let $m = 2$ and $K = \begin{pmatrix} 5 & 9 \\ 5 & 10 \end{pmatrix}$. The matrix K is invertible since the determinant of K is relatively prime to 26.
- The plaintext 'danger' leads to the blocks $3 \;\; 0 \,|\, 13 \;\; 6 \,|\, 4 \;\; 17$. Multiplying each block by K yields $15 \;\; 1 \,|\, 17 \;\; 21 \,|\, 1 \;\; 24$, leading to the ciphertext 'PBRVBY'.
- We'll illustrate in class how to compute the matrix K^{-1}.

Permutation Cipher

- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, and $\mathcal{K}$ is the set of permutations of $\{1, 2, \ldots, m\}$.
- The key is a permutation π. The plaintext is divided into blocks $x_1 x_2 \ldots x_m$ of length m, and the ciphertext for that block is $x_{\pi(1)} x_{\pi(2)} \ldots x_{\pi(m)}$.
- Let $m = 5$, and let π be the following permutation of $\{1, 2, 3, 4, 5\}$:

x	1	2	3	4	5
$\pi(x)$	3	5	4	2	1

- If the plaintext is ‘iliketoeatapplesandbananasandgrapes’, we have

i l i k e	t o e a t	a p p l e	s a n d b	a n a n a	s a n d g	r a p e s
I E K L I	E T A O T	P E L P A	N B D A S	A A N N A	N G D A S	P S E A R

Synchronous Stream Ciphers

- $\mathcal{P}$, $\mathcal{C}$, and $\mathcal{K}$ are defined as before.
- $\mathcal{L}$ represents the keystream alphabet
- g is a keystream generator, i.e. g takes the key K as input and produces a stream $z_1 z_2 z_3 \ldots$ where each $z_i \in \mathcal{L}$.
- For each $z \in \mathcal{L}$, there is an encrypting function $e_z : \mathcal{P} \rightarrow \mathcal{C}$ and a corresponding decrypting function $d_z : \mathcal{C} \rightarrow \mathcal{P}$.
- Here, 'synchronous' means that the value of the stream depends only on K and not on the plaintext.
- The Vigenère Cipher can be thought of as an example of a synchronous stream cipher.

Non-synchronous Stream Ciphers

- $\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$, and $\mathcal{L}$ are defined as before.
- In this case, the stream $z_1 z_2 z_3 \ldots$ can depend on K and on the plaintext used.
- In the Autokey Cipher, one takes $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$. If the plaintext is
$$x_1 x_2 x_3 \ldots,$$
then the stream used for encryption is
$$(K, x_1, x_2, x_3, \ldots).$$
- The encryption function in the Autokey Cipher is compontentwise modular addition.

Example of the Autokey Cipher

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$.
- Suppose that $K = 7$ and the plaintext is 'meetatfour'.
- We have

	m	e	e	t	a	t	f	o	u	r
x	12	4	4	19	0	19	5	14	20	17
z	7	12	4	4	19	0	19	5	14	20
$e_z(x)$	19	16	8	23	19	19	24	19	8	11
	T	Q	I	X	T	T	Y	T	I	L