Q & A session 16 Nov 2020

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Hill cipher (slide from Historical ciphers II)

- This system uses matrices. There is a system parameter n
- First encode the letters into numbers in $[0, 25]$.

Hill cipher (slide from Historical ciphers II)

- This system uses matrices. There is a system parameter n
- First encode the letters into numbers in $[0, 25]$.
- The secret key S is an $n \times n$ matrix over $\mathbb{Z}/26$ which is invertible.
- Write the plaintext a as vector

$$(m_1, m_2, \ldots, m_n) \in (\mathbb{Z}/26)^n.$$

- m gets encrypted into ciphertext

$$c^T = Sm^T.$$

- To decrypt compute

$$m^T = S^{-1}c^T.$$

Hill cipher (slide from Historical ciphers II)

- This system uses matrices. There is a system parameter n
- First encode the letters into numbers in $[0, 25]$.
- The secret key S is an $n \times n$ matrix over $\mathbb{Z}/26$ which is invertible.
- Write the plaintext a as vector

$$(m_1, m_2, \ldots, m_n) \in (\mathbb{Z}/26)^n.$$

- m gets encrypted into ciphertext

$$c^T = Sm^T.$$

- To decrypt compute

$$m^T = S^{-1}c^T.$$

- The inverse of S is computed in $\mathbb{Z}/26$, so you need to use the extended Euclidean algorithm (XGCD) in addition to linear algebra. For a recap of how XGCD works watch the short video.

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}$$

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} =$$

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} = \begin{pmatrix} 19 \\ 23 \\ 25 \end{pmatrix}$$

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} = \begin{pmatrix} 19 \\ 23 \\ 25 \end{pmatrix}$$

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}$$

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} = \begin{pmatrix} 19 \\ 23 \\ 25 \end{pmatrix}$$

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 15 \\ 19 \\ 14 \end{pmatrix} =$$

Example from exercise 1.6

(a) Let

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Encrypt the text `CRY PTO`

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 17 \\ 24 \end{pmatrix} = \begin{pmatrix} 19 \\ 23 \\ 25 \end{pmatrix}$$

$$M = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 3 & 1 \end{pmatrix} \begin{pmatrix} 15 \\ 19 \\ 14 \end{pmatrix} = \begin{pmatrix} 11 \\ 22 \\ 8 \end{pmatrix}$$

This means that the message gets encrypted to `TXZ LWI`.

Example from exercise 1.6

(b) Let M be a 2×2 matrix.
You know that $(1, 3)$ was encrypted as $(-9, -2)$ and that $(7, 2)$ was encrypted as $(-2, 9)$. Find the secret key M.

Let the secret matrix be $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The plaintext-ciphertext pairs define 4 linear equations in the 4 unknowns a, b, c, d as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 1a + 3b \\ 1c + 3d \end{pmatrix} = \begin{pmatrix} -9 \\ -2 \end{pmatrix}.$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 7 \\ 2 \end{pmatrix} = \begin{pmatrix} 7a + 2b \\ 7c + 2d \end{pmatrix} = \begin{pmatrix} -2 \\ 9 \end{pmatrix}.$$

Focus on rows 2 and 4; use 1 and 3 yourself to answer the Canvas quiz.

$1c + 3d = -2 \Rightarrow c = -2 - 3d$; insert into row 4

$7(-2 - 3d) + 2d = -14 + 7d = 9$, thus $7d \equiv 23 \bmod 26$.

Next page: $7^{-1} \equiv -11 \bmod 26$, thus $d = -11 \cdot 23 \equiv 7 \bmod 26$.

Finally: $c = -2 - 3d = -2 - 3 \cdot 7 = -23 \equiv 3 \bmod 26$

Inversion of 7 mod 26

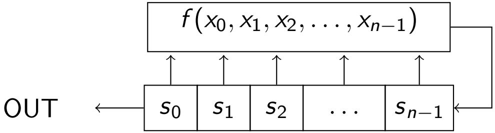
Please watch the XGCD video and read the slides to make sense of this.
Here are the computations we did

26	1	0	
7	0	1	3
5	1	-3	1
2	-1	4	2
1	3	-11	2
0			

This means that $1 = 3 \cdot 26 - 11 \cdot 7$ (yes, indeed $1 = 78 - 77$)

Thus $1 = 3 \cdot 26 - 11 \cdot 7 \equiv -11 \cdot 7 \bmod 26$, i.e., $7^{-1} \equiv -11 \bmod 26$.

Feedback shift registers



Typically $s_i \in \mathbb{F}_2$
Starting state:
$(s_0\, s_1\, s_2\, \ldots\, s_{n-1})$

First output:
s_0
Second state:
$(s_1\, s_2\, \ldots\, s_{n-1}\, f(s_0, s_1, s_2, \ldots, s_{n-1}))$

First $n+2$ outputs:
$s_0\, s_1\, s_2\, \ldots s_{n-1}\, f(s_0, s_1, s_2, \ldots, s_{n-1})\, f(s_1, s_2, \ldots, s_{n-1}, f(s_0, s_1, s_2, \ldots, s_{n-1}))$

To use an FSR as a stream cipher, make $f = f_k$ a function of the key k, put $IV = (s_0\, s_1\, s_2\, \ldots\, s_{n-1})$, and discard the first n output bits.

The attacker sees IV, does not know what the function f is.
For LFSRs the attacker can recover the whole function from $n-1$ output bits (beyond the IV). See the "Security considerations" slide.
But the attacker shouldn't see the output stream anyways!
The ciphertext is the message + output stream (omitting the first n bits).

Encryption with stream cipher

In general, see the Stream ciphers I video & slides.

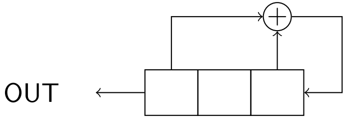
The starting assumption is that Alice and Bob share some secret string k, their key. We will later learn how they can get to this.
Use the key to define f; for LFSRs put $k = c_1 c_2 \dots c_{n-1}$ and $c_0 = 1$.

To encrypt a message m of length ℓ pick a random IV of length n and put $S_0 = IV$. Run the (L)FSR for $n + \ell$ steps, discard the first n output bits (these equal the IV).
Then add the message to the remaining stream $(s_n s_{n+1} s_{n+2} s_{n+3} \dots s_{n+\ell-1})$ to get the ciphertext (one bit at a time).
Send IV and ciphertext.

To decrypt, put $S_0 = IV$, compute $n + \ell$ steps of the (L)FSR, discard the first n output bits, and decrypt by adding the remaining stream to the ciphertext to get the plaintext.

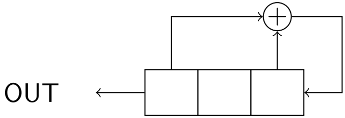
LFSR example

Example $f(x_0, x_1, x_2) = x_0 + x_2$,
aka $s_{j+3} = s_j + s_{j+2}$.
Thus $c_0 = 1, c_1 = 0, c_2 = 1,\ n = 3$.



LFSR example

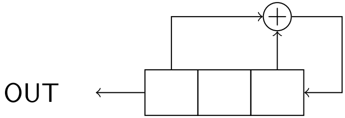
Example $f(x_0, x_1, x_2) = x_0 + x_2$,
aka $s_{j+3} = s_j + s_{j+2}$.
Thus $c_0 = 1, c_1 = 0, c_2 = 1,\ n = 3$.



$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$ The last column gets the coefficients, c_0 on top, c_{n-1} at the bottom.

LFSR example

Example $f(x_0, x_1, x_2) = x_0 + x_2$,
aka $s_{j+3} = s_j + s_{j+2}$.
Thus $c_0 = 1, c_1 = 0, c_2 = 1,\ n = 3$.

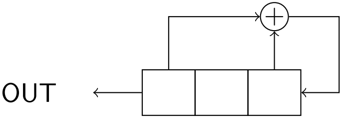


$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$ The last column gets the coefficients, c_0 on top, c_{n-1} at the bottom.

$$\det(xI - C) = \det(xI + C) = \begin{vmatrix} x & 0 & 1 \\ 1 & x & 0 \\ 0 & 1 & x+1 \end{vmatrix}$$

LFSR example

Example $f(x_0, x_1, x_2) = x_0 + x_2$,
aka $s_{j+3} = s_j + s_{j+2}$.
Thus $c_0 = 1, c_1 = 0, c_2 = 1,\ n = 3$.



$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$ The last column gets the coefficients, c_0 on top, c_{n-1} at the bottom.

$$\det(xI - C) = \det(xI + C) = \begin{vmatrix} x & 0 & 1 \\ 1 & x & 0 \\ 0 & 1 & x+1 \end{vmatrix}$$

Use Cramer's rule to compute the determinant:

$$\begin{aligned} \det(xI + C) &= x \cdot x \cdot (x+1) + 1 \cdot 1 \cdot 10 \cdot 0 \cdot 0 - (1 \cdot x \cdot +0 \cdot 1 \cdot x + (x+1) \cdot \\ &= x^3 + x^2 + 1 + 0 - (0) = x^3 + x^2 + 1. \end{aligned}$$

In the video I prove that the characteristic polynomial equals $x^n - \sum_{i=0}^{n-1} c_i x^i$, so you can just use this formula.