Lecture 11

Definition: A *stream cipher* combines plaintext $p_1p_2\cdots p_n$, with a keystream $k_1k_2\cdots k_n$, to get ciphertext $c_1c_2\cdots c_n$. In a stream cipher the plaintext digits are encrypted one at a time.

Autokey Cipher (1585)

- Start by picking a seed φ which is a single letter.
- Given the plaintext $p_1p_2\cdots p_n$ we get a keystream $k_1k_2\cdots k_n$ by:

$$k_1 = \varphi, k_2 = p_1, \ldots, k_n = p_{n-1}$$

- The encoding function:

$$C_i \equiv E_{k_i}(p_i) \equiv p_i + k_i \pmod{26}$$

produces the ciphertext $c_1c_2\cdots c_n$.

- The decoding function is:

$$D_{k_i}(c_i) \equiv c_i - k_i \pmod{26}$$

$D_{k_i}(c_i) \equiv p_i + k_i - k_i \equiv p_i \pmod{26}$

- The kibitzer can attack the autokey cipher by trying every seed.

Example 1: Using the autokey cipher play the role of the sender and receiver.

a) With the seed D encode the plaintext "M E D I A"

12 4 3 8 0

$E(M) \equiv E(12) \equiv 12+3 \equiv 15 \pmod{26}$ → P
$E(E) \equiv E(4) \equiv 4+12 \equiv 16 \pmod{26}$ → Q
$E(D) \equiv E(3) \equiv 3+4 \equiv 7 \pmod{26}$ → H
$E(I) \equiv E(8) \equiv 8+3 \equiv 11 \pmod{26}$ → L
$E(A) \equiv E(0) \equiv 0+8 \equiv 8 \pmod{26}$ → I

The ciphertext is PQHLI

b) With the seed B decode the ciphertext "G F M A I M"

6 5 12 0 8 12

$D(G) \equiv 6-1 \equiv 5 \pmod{26}$ → F
$D(F) \equiv 5-5 \equiv 0 \pmod{26}$ → A
$D(M) \equiv 12-0 \equiv 12 \pmod{26}$ → M
$D(A) \equiv 0-12 \equiv -12 \equiv 14 \pmod{26}$ → O
$D(I) \equiv 8-14 \equiv -6 \equiv 20 \pmod{26}$ → U
$D(M) \equiv D(12) \equiv 12-20 \equiv -8 \equiv 18 \pmod{26}$ → S

The ciphertext is FAMOUS

Vernam Cipher (1917)

- Letters are converted into their binary equivalent:

A	B	C	D	E	F	G	H	I
00000	00001	00010	00011	00100	00101	00110	00111	01000

J	K	L	M	N	O	P	Q	R
01001	01010	01011	01100	01101	01110	01111	10000	10001

S	T	U	V	W	X	Y	Z
10010	10011	10100	10101	10110	10111	11000	11001

- By picking a keystream in binary $k_1k_2\cdots k_n$ the same length as the plaintext in binary $p_1p_2\cdots p_n$ the encoding function:

$$c_i \equiv E_{k_i}(p_i) \equiv p_i + k_i \pmod 2$$

produces the ciphertext $c_1c_2\cdots c_n$.

$D_{k_i}(c_i) \equiv c_i + k_i$
$\equiv p_i + k_i + k_i$
$\equiv 0 \pmod 2$
$\equiv p_i \pmod 2$

- The decoding function is:

$$D_{k_i}(c_i) \equiv c_i + k_i \pmod 2$$

- When a keystream is completely random and is used only once the Vernam cipher is unbreakable. This means someone with only the ciphertext (the kibitzer) can only guess what the plaintext is.

Example 2. Using the Vernam cipher play the role of the sender and receiver.

a) Encode "RICH": 10001 01000 00010 00111
using the keystream: 00100 00100 11011 11011

10101 01100 11001 11100

b) Decode: 00111 00000 11011 11000
using the keystream: 00100 00100 11011 11011

00011 00100 00000 00011
D E A D

plaintext DEAD

The RSA Cryptosystem (1977)

- Choose two prime numbers p, q and let $m = pq$, $n = (p-1)(q-1)$.
- Pick an encoding power e so that $0 \leq e < n$ and e has an inverse in mod n.
- Pick a decoding power d so that $0 \leq d < n$ and $e \cdot d \equiv 1 \pmod{n}$.
- The encoding function is:
$$E(x) \equiv x^e \pmod{m}$$
- The decoding function is:
$$D(x) \equiv x^d \pmod{m}$$
- In each of the previous ciphers discussed the encoding function is kept secret. In the RSA cryptosystem the encoding function is made known to the kibitzer. This type of cryptosystem is called a *public key cryptosystem.*
- The RSA cryptosystem is extremely secure when p and q are very large (and carefully chosen). In this case, it is next to impossible for the kibitzer to find $D(x)$ from $E(x)$.

Example 3. Dr. Ecco, Professor Scarlet and Evangeline have set up the following RSA cryptosystem:

	Private Information	Public Information	
Evangeline	$p = 3,\ q = 7$	$E(x) \equiv x^5 \pmod{21}$	$n = 2 \cdot 6 = 12$
Professor Scarlet	$p = 3,\ q = 13$	$E(x) \equiv x^5 \pmod{39}$	$n = 3 \cdot 12 = 24$
Dr. Ecco	$p = 53,\ q = 101$	$E(x) \equiv x^3 \pmod{5353}$	$n = 52 \cdot 100 = 5200$

a) Why can't Dr. Ecco use an encoding power of 5?

$n = (p-1)(q-1) = 52 \cdot 100 = 5200$

and 5 & 5200 are not relatively prime

So 5 has no inverse mod 5200.

b) Dr. Ecco would like to send Evangeline the secret message "R U N". Find the ciphertext:
17 20 13

$p = 3,\ q = 7$ so $m = 21,\quad n = (p-1)(q-1) = 2 \cdot 6 = 12$

$E(x) \equiv x^5 \pmod{21}$

$E(R) \equiv (17)^5 \equiv ((-4)^2)^2(-4) \equiv 16^2(-4) \equiv (-5)^2(-4)$

$\equiv 25(-4) \equiv (4)(-4) \equiv -16 \equiv 5 \pmod{21}$

$\boxed{E(R) \equiv 5 \pmod{21}}$

$E(U) \equiv (20)^5 \equiv (-1)^5 \equiv -1 \equiv 20 \pmod{21}$

$\boxed{E(U) \equiv 20 \pmod{21}}$

$E(N) \equiv (13)^5 \equiv (-8)^4(13) \equiv (64^2) \cdot 13 \equiv 1^2 \cdot 13 \equiv 13 \pmod{21}$

$\boxed{E(N) \equiv 13 \pmod{21}}$

Ciphertext is $\boxed{F\ U\ N}$

c) What is Evangeline's (private) decoding function?

$p = 3$, $q = 7$, $m = p \cdot q = 21$, $n = (p-1)(q-1) = 2 \cdot 6 = 12$

$e = 5$ want $d \cdot e \equiv 1 \pmod{12}$

$5 \cdot 5 \equiv 25 \equiv 1 \pmod{12}$ so we take $\underline{d = 5}$

The decoding function is

$$D(x) \equiv x^5 \pmod{21}$$

d) Show how Evangeline recovers the plain text from the ciphertext found in part b).

Ciphertext was F U N
5 20 13

$D(x) \equiv x^5 \pmod{21}$

$D(F) = D(5) \equiv 5^5 \equiv (5^2)^2 \cdot 5 \equiv 25^2 \cdot 5$

$\equiv 4^2 \cdot 5 \equiv 16 \cdot 5 \equiv (-5) \cdot 5 \equiv -25 \equiv 17 \pmod{21}$

$D(F) \equiv 17 \pmod{21}$ R

$D(U) = D(20) \equiv (20)^5 \equiv (-1)^5 \equiv -1 \equiv 20 \pmod{21}$

$D(U) \equiv 20 \pmod{21}$ U

$D(N) \equiv D(13) \equiv (13)^5 \equiv (-8)^5 \equiv 64^2 \cdot 8 \equiv 1 \cdot 13 \equiv 13 \pmod{21}$

$D(N) \equiv 13 \pmod{21}$ N

So the plaintext was R U N

Lecture 12: Things to come.

Induction + Recursion

Principle of Mathematical Induction

Given a statement P concerning the positive integers, such that:

(i) $P(1)$ is true,

(ii) for each $n \geq 1$, whenever $P(n)$ is true this implies $P(n+1)$ is true.

Then P is true for all positive integers.

Note: The principle of mathematical induction and the Well-Ordering property for the positive integers are logically equivalent.

Neither can be proven from the integer axioms (i.e. $\mathbb{Z}$ is an integral domain) + the order properties of the integers.

- One must be taken as an axiom, the other proven as a theorem.