

Math Club

Cryptography

1 Simple Ciphers

The first types of ciphers used were called Caesar shifts. You simply shift every letter by a given number. For example a Caesar shift of 5 says replace “A” with “F,” “E” with “J,” and so on until “Z” is replaced with “E.”

In mathematical language, once we replace the letters A,B,C, and so on with numbers 0,1,2, then the encryption function is

$$f(x) = x + 5 \text{ mod } 25.$$

This type of cipher is very easy to break.

Then next type of cipher was the substitution cipher. Instead of just shifting the alphabet, you assign them different letters or symbols.

This is also an easy cipher to break with frequency analysis. Mary Queen of Scots found this out the hard way. See <http://www.math.utah.edu/~ko-revaar/ACCESS2006/Tuesdaydocs/> for some maple worksheets to do frequency analysis.

There were many other types of ciphers like the enigma machine, using Navaho code talkers, using cipher disks, etc.

Main Problem: Key distribution, and if you know how to encode something, you know how to decode it.

2 Public Key Cryptography

Mathematicians wanted to find a way you could give the encryption method to everyone, but only you would know how to decrypt.

The most famous of the public key cryptography methods is RSA, named after the “inventors” Ronald Rivest, Adi Shamir, and Leonard Adleman.

This method is based on the fact that it is easy to multiply but hard to factor.

2.1 RSA

First Alice sets up to receive messages.

1. Alice picks two (large) primes p and q .
2. Alice computes her modulus $N = pq$. This is her first piece of her public key.
- 2a Alice privately computes an auxiliary modulus $N_2 = (p - 1)(q - 1)$. She keeps this secret
3. Now Alice finds a value e such that e is relatively prime to N_2 , i.e., $\gcd(e, N_2) = 1$.
- 3a Now Alice finds a value d such that $ed \equiv 1 \pmod{N_2}$. She does this by using Euclid's Algorithm.
See <http://www.math.byu.edu/chamberlain/Access/ClockArithmetic.pdf> for notes on Euclid's Algorithm.
4. Alice is now ready for people to send her messages. She gives e and N to everybody and tells them to break up their message into packets no bigger than N and encrypt the packets M according to the function

$$E(M) \equiv M^e \pmod{N}.$$

5. Now Bob wants to send Alice a message. He converts his message to numbers, and breaks the big number message into packets that are smaller than N that Alice gave him.
- 5a. Bob determines $y = E(M)$ and sends y it to Alice.
6. Mr. Evil intercepts y , but he doesn't know Alice's d , so he can't figure out what the message is.
7. Alice now computes $D(y) \equiv (y)^d \pmod{N}$ to get back to M .

Facts:

- Finding e and d is easy if you know p and q .
- It is impossible to find d if you only know e and N .

For added security, use a secure signature.

2.1.1 SECURE SIGNATURE

Do these instructions at the appropriate place in the above instructions.

- 5'. Bob converts his message into a large number. But Bob has also created his own public key e_B, N_B and private key d_B . He thinks of a sensible "signature" and makes it numeric s_B . He decrypts this using his private key to get $D_B(s_B)$.
- 5'a. Bob appends the decrypted signature to his numerical message he wants to send to Alice and breaks this into packets which are smaller than Alice's N . Then he encrypts this using Alice's public key, and sends this to Alice.
- 6'. Mr. Evil intercepts y , but he doesn't know Alice's d , so he can't figure out what the message is, and he can not forge Bob's signature to try to give Alice a false message.
- 7'. Alice now computes $D(y)$ and gets the message M with a bunch of gibberish tacked on at the end which she knows is Bob's signature. She uses Bob's public key to encrypt the gibberish to read his "signature."

3 The Mathematics Behind It All

This method is based on three Theorems from Number Theory.

Theorem 1 (The Division Algorithm) *Given any integers a and b , with $a > 0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r < a$. If a does not divide b , then r satisfies the stronger inequalities $0 < r < a$.*

Theorem 2 (The Euclid Algorithm) *Given integers b and $c > 0$, we make a repeated application of the division algorithm to obtain a series of*

equations

$$\begin{aligned}
 b &= cq_1 + r_1, 0 < r_1 < c, \\
 c &= r_1q_2 + r_2, 0 < r_2 < r_1, \\
 r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2, \\
 &\dots \\
 r_{j-2} &= r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}, \\
 r_{j-1} &= r_jq_{j+1}.
 \end{aligned}$$

The greatest common divisor $\gcd(b, c)$ of b and c is r_j , the last nonzero remainder in the division process. Values of x_0 and y_0 in $\gcd(b, c) = bx_0 + cy_0$ can be obtained by writing each r_i as a linear combination of b and c .

Theorem 3 (Fermat's Little Theorem) Let p be a prime and a an integer such that p does not divide a . Then $a^{p-1} \equiv 1 \pmod p$.

Corollary 1 Let p and q be primes and n any integer. Then $x^{n(p-1)(q-1)+1} \equiv x \pmod{pq}$.

4 Converting Letters to Numbers

From Tom Davis' notes:

	0	1	2	3	4	5	6	7	8	9
0	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
1	SP	A	B	C	D	E	F	G	H	I
2	J	K	L	M	N	O	P	Q	R	S
3	T	U	V	W	X	Y	Z	a	b	c
4	d	e	f	g	h	i	j	k	l	m
5	n	o	p	q	r	s	t	u	v	w
6	x	y	z	.	,	:	;	'	"	'
7	!	@	#	\$	%	^	&	*	-	+
8	()	[]	{	}	?	/	<	>
9	0	1	2	3	4	5	6	7	8	9

The entries with XX are not used, and "SP" is the space character. Thus all characters code to between 10 and 99. For example "U" is 31 and "5" is 95. Also if we wanted to encode "C3PO" we would get 13932625.

5 Error Detection Codes

There are some instances when you want to know if a code has been tampered with. For example forged driver's licenses.

Utah assigns an eight-digit driver's license number in sequential order, and then puts a special digit at the end. This special last number is found so that the dot product of the number with the vector $(9,8,7,6,5,4,3,2,1)$ is $0 \pmod{10}$. This makes it easy for officials to find forgeries. This method detects 90.1% single-digit errors and 100% of all transposition errors. A notable transposition error occurred when Lt. Col. Oliver North gave the U.S. Assistant Secretary of State Elliot Abrams an incorrect Swiss bank account number for depositing \$10 million for the Contras. Oops.

Other states have ways of encoding first, middle and last names as well as sex and birth day, month and year.

6 Further Reading

The Code Book by Simon Singh

The Theory of Numbers by Niven, Zuckerman, and Montgomery

Tom Davis' notes on Cryptography are located at
<http://mathcircle.berkeley.edu/BMC3/crypto.pdf>

Assigning Driver's License Numbers by Joseph A. Gallian, Mathematics Magazine, Vol. 64, No. 1 (Feb., 1991), pp. 13-22. You can find this at
<http://www.jstor.org/pss/2690449>

7 Activity

Do the following:

1. Go to 149 TMCB. It's a computer lab where we will make our own encryption code.
2. Open Firefox (NOT Netscape).
3. Go to the following web address:
<https://math.byu.edu/info/mathclub.php>
4. Click on the link for RSA Maple Worksheet.

5. Copy the URL.
6. Open Maple.
7. Open a URL file.
8. Paste the URL into the box.
9. Help others around you who might not be there yet.