

MATH 100 - NOTES ON CRYPTOGRAPHY

The basic idea of *cryptology* is that Alice wants to send a message to Bob, in such a way that Bob can decode the message when he receives it, but if Mr. X intercepts the message he cannot translate it. We start with one of the simplest general types, *monoalphabetic substitution ciphers*, which refers to any method wherein Alice substitutes each letter of the alphabet by another letter. This can be done by changing the letters a, \dots, z to numbers $0, \dots, 25$, using an arithmetic function that is a permutation on \mathbb{Z}_{26} , and then changing back to letters. This allows the method to be automated, and to be varied by changing the parameters.

There are many more sophisticated ciphers, but the best ones still use arithmetic in the integers modulo n , though for a much, much larger number n , and for blocks of symbols rather than single letters.

For reference, here is an enumeration of the Roman alphabet.

01	23	45	67	89	1011	1213	1415	1617	1819	2021	2223	2425
<i>AB</i>	<i>CD</i>	<i>EF</i>	<i>GH</i>	<i>IJ</i>	<i>KL</i>	<i>MN</i>	<i>OP</i>	<i>QR</i>	<i>ST</i>	<i>UV</i>	<i>WX</i>	<i>YZ</i>

We will consider four basic ciphers, followed by a brief discussion of some more sophisticated ones.

- A *Caesar shift* uses the function $f(x) = x + b \pmod{26}$ for some b .
- An *affine code* uses the function $f(x) = ax + b \pmod{26}$ for some pair a, b with $\gcd(a, 26) = 1$.
- A *keyword cipher* uses a keyword and key letter to mix up a Caesar shift.
- A *Vigenère cipher* uses a keyword and a square 26×26 array for encryption and decryption.

esection*Resources

Albrecht Beutelspacher, *Cryptography*, published by MAA.

Fred Cohen:

all.net.com/books/ip/Chap2-1.html

Wikipedia:

en.wikipedia.org/wiki/History_of_cryptography

Trinity College (Conn.) Computer Science Department:

starbase/trincoll.edu/%7Ecrypto/

Kent D. Boklan:

razorpoint.com/Rz.ConfederateCode.pdf