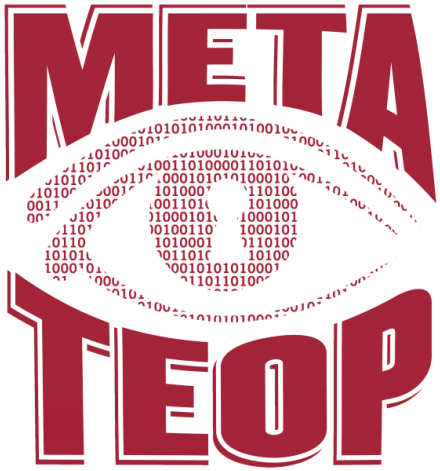
META-TEOP

Cryptography Workshop

Dr. Mark Farag

Mathematics Enrichment Through Applications
Technical Enrichment and Outreach Program
Sponsored by the MAA Tensor-SUMMA Program



FAIRLEIGH
DICKINSON
UNIVERSITY

META-TEOP Cryptography Workshop

A Brief History of Cryptography and an Introduction to Ciphers

Mark Farag
(mfarag@fdu.edu)
Mathematics Program
Gildart Haase School of Computer Sciences and Engineering
Fairleigh Dickinson University

What is Cryptography?

We distinguish between these related concepts:

1) *Cryptography*: the study of techniques to keep information secure

2) *Cryptanalysis*: the study of how to defeat cryptographic methods

3) *Cryptology*: the study of cryptography and cryptanalysis

Cryptography in Antiquity

Some past civilizations that exhibited elements of cryptography:

1) *Old Kingdom of Egypt* (c. 1900 BC): on monuments; of unclear purpose

2) *Mesopotamia* (c. 1500 BC): on clay tablets; even used to hide trade secrets (like pottery glaze recipes)

3) *Greece*: varied use; even appeared in the *Iliad*!

Caesar Ciphers

(BFYHM TZY KTW GWZYZX)

Although these are simple enough to be taught to school children today, they were used by Julius Caesar (c. 60 BC) for secret military communications.

They rely on a shift of the standard alphabet:

$$
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\
\hline
\Updownarrow & \Updownarrow \\
\hline
D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C \\
\hline
\end{array}
$$

Radio Orphan Annie Codes

Radio Orphan Annie Codes
(a.k.a. Simple Substitution Ciphers)
(20,3,9,1,6,1,23,11,25,15,24,8,25,14,20,12,16)

These are more general than Caesar ciphers - the idea is no longer just to shift the alphabet, but rather to create a more random correspondence between letters.

These have been in existence for quite some time (at least since the Middle Ages); they were popularized on the Orphan Annie radio show in the 1930s.

Children who listened to the show would join Radio Orphan Annie's Secret Society by sending away for their decoder badge or pin. At the end of each episode, they could decode a secret message with it.

Simple Decoder

Here is a simplified version of the decoder[1]:

Example: 8,20,17,12,22,21,14,24,11,26,17,12,13
(Key: P)

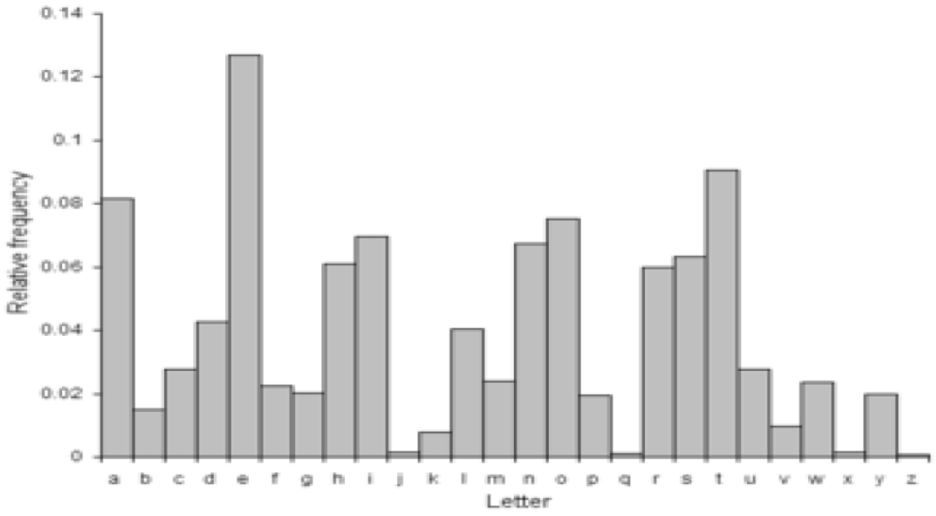
How easy is this code to "crack" when the decoder is known?

Simple Decoder

Answer: Just try the 26 different "key" positions until the encoded messages makes sense.

How easy is the code to "crack" when the decoder is unknown?

Answer: This is harder, but it is possible with frequency analysis[2]:



Hill Ciphers

Into the 20th Century (Hill Ciphers)

For these ciphers we use matrices, which are ordered arrays of numbers like:

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

We may multiply matrices "row by column":

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} ae + bf \\ ce + df \end{pmatrix}$$

We may then take an English message, translate it into its numerical equivalent, and use the matrix to encode the numbers in pairs:

The message: HILL CIPHER

Hill Ciphers

Numerical equivalent: 8, 9, 12, 12, 3, 9, 16, 8, 5, 18

Take the first pair (8,9) and encode with the matrix above:

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 2(8)+1(9) \\ 1(8)+1(9) \end{pmatrix} = \begin{pmatrix} 25 \\ 17 \end{pmatrix}$$

So what? If the matrix has an "inverse" (another matrix that reverses the operations to return the original numbers), then we may decode the encoded part of the message (25,17). For this matrix, the inverse is:

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$$

Multiply to see that it works!

Hill Ciphers

$$\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} 25 \\ 17 \end{pmatrix} = \begin{pmatrix} 1(25) + (-1)(17) \\ (-1)(25) + 2(17) \end{pmatrix} = \begin{pmatrix} 8 \\ 9 \end{pmatrix}$$

How to determine such inverses is studied in a subject called Linear Algebra:

If a, b, c, d are numbers for which $D := ad - bc \neq 0$, then the 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, has inverse $\begin{pmatrix} \frac{d}{D} & -\frac{b}{D} \\ -\frac{c}{D} & \frac{a}{D} \end{pmatrix}$.

Can you prove this? What happens when $D = 0$?

What is the inverse of $\begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$?

Will something similar work for 3×3 matrices?

Hill Ciphers

Even such ciphers are not too difficult to crack with frequency analysis on pairs of letters.

More modern techniques (such as DES and RSA) are studied in a subject called Cryptography.

These subjects are not just for fun; they are used for secure financial transactions, communications, and military and intelligence operations (see, e.g., www.nsa.gov).

References

[1]: http://www.radioarchives.org/annie/

[2]: http://en.wikipedia.org/wiki/Frequency_analysis

48, 28, 15, 10, 32, 18

Basic Cryptographic Protocols

META-TEOP Cryptography Workshop

Basic Cryptographic Protocols

Mark Farag
(mfarag@fdu.edu)
Mathematics Program
Gildart Haase School of Computer Sciences and Engineering
Fairleigh Dickinson University

Cryptographic Protocols

1. The Big Picture

Textbooks often use Alice and Bob to represent two parties involved in message exchanges. The situation we consider is as follows:

1) Alice and Bob wish to exchange a secret key to encrypt/decrypt messages.
2) Alice and Bob may not even know each other.
3) Alice and Bob are communicating over a public network.

How can Alice and Bob set up their secret key exchange over the public network?

Diffe-Hellmann Key Exchange

Suppose Alice and Bob agree on an invertible matrix M for a Hill cipher (note that this is done in public). Then they can generate a shared secret key for communication over the public network as follows:

1) Alice chooses a random positive integer a and computes M^a.
2) Bob chooses a random positive integer b and computes M^b.
3) Alice sends Bob M^a and Bob sends Alice M^b over the public network.
4) Alice and Bob both compute their shared secret key: $A = M^{ab} = (M^a)^b = (M^b)^a$.

Important Questions

What does an eavesdropper, Eve, see over the network?

In general, why can't Eve compute A easily from this information?

What if we now add another person, Carol, to the group? How can we modify this key exchange so that all three have a common secret key at the end? Assume that M is still the agreed-upon initial matrix.

Solution

1) Alice chooses a random positive integer a and computes M^a, which she sends to Bob.
2) Bob chooses a random positive integer b and computes $(M^a)^b = M^{ab}$, which he sends to Carol.
3) Carol chooses a random positive integer c and computes $(M^{ab})^c = M^{abc}$.
4) Carol then computes M^c and sends it to Alice.
5) Alice computes M^{ac} and sends it to Bob.
6) Bob computes M^{abc}.
7) Bob computes M^b and sends it to Carol.
8) Carol computes M^{bc} and sends it to Alice.
9) Alice computes M^{abc}.

Now they all have a shared secret key $A = M^{abc}$.

Authentication

The authentication problem occurs in different forms. Let's start with the following version:

In order to get on the Internet in the first place, Alice needs to log on to some host device (laptop, smart phone, etc.). How can Alice verify her identity to the device?

The standard solution is to use a password. It is not a good idea to have an unencrypted version of the password stored on the device in case it is compromised, so a *one-way function* is often employed. A one-way function f is a function such that:

a) for a given input x, $f(x)$ is relatively easy to compute, and
b) given f and $f(x)$, x is difficult to compute.

Brief Excursion Into Number Theory

META-TEOP Cryptography Workshop

A Brief Excursion into Number Theory

Mark Farag
(mfarag@fdu.edu)
Mathematics Program
Gildart Haase School of Computer Sciences and Engineering
Fairleigh Dickinson University

Basic Number Theory

Number theory is the study of the integers and their properties. You are probably already familiar with some of the basic notions. For example:

Definition: A *prime number* is an integer $p > 1$ whose only positive integer divisors are 1 and p.

Definition: The *greatest common divisor* of two nonzero integers is the largest positive number that evenly divides both integers.

Definition: Two integers are *relatively prime* if their greatest common divisor is 1.

Modular or "Clock" Arithmetic

A useful kind of arithmetic on the integers arises as follows:

Fix an integer $n > 1$. Then for any integers a and b, we define $a + b \pmod{n}$ as the remainder obtained by dividing $a + b$ by n.

You are used to arithmetic modulo 12: starting at 11 o'clock and adding 3 hours brings you to 2 o'clock.

We are going to use arithmetic modulo a certain number that arises as follows:

Definition: Given a positive integer m, $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m. We refer to ϕ as the *Euler totient function*.

RSA Encryption

META-TEOP Cryptography Workshop

RSA Encryption

Mark Farag
(mfarag@fdu.edu)
Mathematics Program
Gildart Haase School of Computer Sciences and Engineering
Fairleigh Dickinson University

The Idea Behind RSA Encryption

1) RSA is an acronym for Rivest, Shamir, Adleman.

2) This encryption method is the current standard for many common web browsers.

3) The method is a **public-private key** system – two parties who may not know and may not trust each other can communicate privately over a public network.

4) The method's security is closely tied to the difficulty of factoring large numbers and/or computing logarithms modulo a positive integer n.

RSA Algorithm

1) Construct $n = pq$, where $p \neq q$ are primes.

2) Compute $\phi(n)$.

3) Choose an integer $1 < e < \phi(n)$ that is relatively prime to $\phi(n)$.

4) Compute $d = e^{-1}$ modulo $\phi(n)$.

Here, n and e constitute the public key, while d is kept as the private key.

Encryption and Decryption

The plaintext should be an integer $0 \leq x < n$.

The ciphertext is computed as $b = x^e$ modulo n.

The plaintext is recovered by $x = b^d = (x^e)^d = x^{ed}$ modulo n.

RSA Example

Let's pick $p = 7$ and $q = 13$ to illustrate the algorithm. Note that these numbers are much too small to be used in practice!

Now $n = pq = 7(13) = 91$, and $\phi(n) = 6(12) = 72$.

The choice of e must be made so that $\gcd(e, 72) = 1$, so e cannot be 2, 3, or 4. However, $e = 5$ is relatively prime to $\phi(n) = 72$. Note that other choices are possible!

Now we want to find the secret key, d, which must satisfy $ed = 1 \bmod 72$. Observe that $d = 29$ satisfies this condition since $5(29) = 145$, which has remainder of 1 upon division by 72.

RSA Example

A message such as $x = 10$ would then by encrypted as $b = x^e = 10^5 \bmod 91$, or $b = 82 \bmod 91$.

To decrypt and recover the plaintext, we calculate $x = b^d = 82^{29}$ modulo 91. This is not as bad as it seems since, modulo 91, we have $82^1 = 82, 82^2 = 81, 82^4 = (82^2)^2 = 81^2 = 9, 82^8 = (82^4)^2 = 9^2 = 81$, and $82^{16} = 81^2 = 9$. So we use this to reduce $82^{29} = (82)^{16}(82)^8(82)^4(82)^1 = (9)(81)(9)(82) = 10$ modulo 91.