On the Science Behind Computing (Part I)

Samir Khuller *

1 Encryption of Data

All modern communication relies on the ability to communicate securely over electronic networks. Data if transmitted openly, may inadvertently fall into the wrong hands and the cost can be staggering - and the cost of not being able to do eCommerce is unimaginable to most of us today.

We start by discussing an extremely simple protocol to communicate that was used by Julius Caesar centuries ago. Caesar wanted to communicate with his generals, and typically the communication was done via men on horses, or runners who would travel quietly at night so as to not be detected. Early methods involved telling the runner the message, but if the runner was captured then they would be tortured until they revealed the message. By writing the message in code, even the runner did not know the message and thus even if they were tortured, they revealed nothing. Caesar used the simple idea of shifting the alphabet; so for example A would be mapped to B, B to C etc. Note that we would use a wrap-around of the text and map Z to A.

Thus a word like "JIMMY" would map to "KJNNZ" (using a shift by 1). However, we can use any shift we like. A shift of 2 would map A to C, B to D etc. Naturally Z would map to B. Caesar and his generals apparently used this method to communicate secretly, and the only reason the code worked was that the enemy assumed that they were communicating in a different language. However, if we knew the scheme we can easily break the code since we can try all the possible shifts (there are only 25 possible interesting shifts).

A better method is to use what is called a substitution cipher. Here each letter of the alphabet is mapped to a unique letter by fixing an arbitrary permutation of the alphabet in advance. The main problem with this is that the secret is the permutation which the decoder may have to memorize which can be non-trivial to do or if the decoding table were to fall into the wrong hands then again that would completely compromise the code. In addition, even these codes are not totally secure, since they are susceptible to frequency attacks. What this means is that if some letter were to occur very frequently in the source text (for example E), then its mapped letter (say X) will occur very frequently. This makes us susceptible to such attacks.

Another scheme is called the Vignere cipher. This uses a collection of Caesar's ciphers with different shifts. For example suppose we use the word "DOG" as our secret key.

We repeat the letter DOG above each letter of the message as follows.

```
DOGD OGDO GD OGDO GDOGDOGD
JOHN WILL BE BACK TOMORROW
```

*Department of Computer Science, University of Maryland, College Park, MD 20742. E-mail : samir@cs.umd.edu.

All the letters below the D will be encrypted using a shift of 3 (mapping A to D). The letters below the O will be shifted using a shift of 14 (mapping A to O), and the letters below the G will be shifted using a shift of 6 (mapping A to G).

Thus we get (after doing the encryption of the letters below the D)

```
DOGD OGDO GD OGDO GDOGDOGD
JOHN WILL BE BACK TOMORROW
M  Q   O   H   F   R  U  Z
```

We now do the encryption of the letters below the O.

```
DOGD OGDO GD OGDO GDOGDOGD
JOHN WILL BE BACK TOMORROW
MC Q K OZ  H P FY  RA UF Z
```

We now do the encryption of the letters below the G to get the final piece of text.

```
DOGD OGDO GD OGDO GDOGDOGD
JOHN WILL BE BACK TOMORROW
MCNQ KOOZ HH PGFY ZRAUUFMZ
```

The main benefit is that the secret word is easy to remember, so we do not need to write it down anywhere and the decoding can be done easily. However note that we have to be careful while using this method, in the sense that even if one letter of the message is lost in transmission, then the decoding will break completely (this is not true in Caesar's cipher). Again, not surprisingly these methods too are not terribly secure. If we guess the length of the secret word (and try all lengths between 1 and 20), then we can use frequency analysis to break the code if we intercept a large amount of communication.

Most modern cryptographic schemes do not use these types of codes, since all these codes involve setting up some sort of "secret" in advance of the communication. However, when we use our credit cards to shop online, we have not set up any secret key with Amazon - so how can we communicate securely with Amazon? The secret lies in a new form of encryption called Public Key Cryptography. One popular scheme in use is called RSA (Rivest, Shamir and Adleman). In this scheme there is a *public key* which is widely distributed (say by Amazon). Anyone can use this key to encrypt a message. Along with the public key is a *private key* that Amazon keeps secret; and only they can decode the message. This is different from most methods where there is only a single key to communicate for a pair of individuals. The security of the code relies on the property that it is hard to factor large numbers (at least there is no known efficient method to do this).