The Three ~Investigators ~

Written by: Sridhar Iyer,
IIT Bombay

"We Investigate Anything", was the motto of the Three Investigators. They called themselves Jupe, Pete and Bob, as in the famous Three Investigators mystery series presented by Alfred Hitchcock. This time they were on the trail of the notorious TRX Gang. The gang had stolen a genetically engineered strain of a micro-organism which was being developed as the source of an anti-HIV drug by the National Research Institute. If the drug were successful, it would be a cure for AIDS and the gang intended to sell it to competing pharmaceutical companies. The micro-organism was in a bio-safety container which could be opened only with a special key. While escaping with the container, the gang had lost the key. The Three Investigators had been called in and they had found the key. Now they had to recover the container from the TRX Gang.

Jupe's quarry was one of the gang members. He had caught sight of the man coming out of a hotel and had followed him to a house in a secluded lane. "It must be their headquarters", mused Jupe. He waited for a while and was wondering whether to approach the house or wait for the man to come out, when a heavy hand fell on his shoulder. A nasty voice said, "All right, you nosey kid. We've got you now." He had fallen into clutches of the gang.

"Give us the key", said the gang leader. "I dont have it with me", cried Jupe, berating himself for getting caught so easily in their trap. "Then write a note to your friends telling them to send you the key. We will let you go once we have the key. Mind you, dont try to be clever or you will regret it", warned the gang leader menacingly.

Jupe had to think quickly to find a way out of this predicament. He recalled that he had once devised a secret communication code for the Three Investigators. Would Pete and Bob remember it? His only hope was that they would understand his secret message.

"Give the key to the messenger who brings this note. I Found My Quarry.", he wrote and handed it to the gang leader. "What is this line - I found my quarry?", asked the gang leader suspiciously. "Pete and Bob know that I was trailing one of your men. They are more likely to give the key if I tell them that I found him.", said Jupe, hoping that message would be allowed to pass. "Looks more like the quarry found you", said the gang leader, laughing at his own wit. He called one of his men and sent him off with the note.

"Why does he want the key in such a hurry?", wondered Bob, when he received the note. "Jupe always has a good reason. He just doesnt tell us. This note is in his writing, so it must be ok.", said Pete going to fetch the key. Bob was still looking at the message when he noticed the letters in the line - I Found My Quarry. It was unlike Jupe to use capital letters for each word in a sentence. He looked at the letters - IFMQ. Like a flash, he realized that Jupe was playing their code game. One person would choose a word and substitute each letter of the word with a different letter, according to some fixed rule. The other person had to reverse the substitution and find the original word. So what was the original word which resulted in IFMQ, after substitution of its letters?

Meanwhile Pete was handing over the key to the messenger. As soon as the messenger had left, Bob said, "Pete, call the police. We need to follow that guy. Jupe needs help". Quickly he explained, "See this IFMQ. Substitute each letter by its previous letter in the alphabet and it spells - HELP." - Jupe caught by the gang and constructing a message.

As you may know, the science of transmitting information in an encoded form so that only an intended recipient can decode the information and reveal its meaning, is called Cryptography. A system for encrypting and decrypting information is called a cryptosystem. A cryptosystem has four components: (i) The 'plain text': This is the information that needs to be sent. In the above story, the plain text is the word 'HELP'. (ii) The 'cipher text': This is the information that is transmitted as a result of encryption. In the above story, the cipher text is 'IFMQ'. (iii) The 'algorithm': This is the rule to be followed for encoding and decoding. In the above story, the encryption algorithm is to substitute each letter of the plain text by its following letter in the alphabet. (iv) The 'key': This is the number known only to the sender and recipient. In the above story, key is 1, since each letter is substituted by its next letter during encryption. If the key had been 2, the resulting cipher text would be 'JGNR', if the key had been 3, the cipher text would be 'KHOS' and so on.

A strong cryptosystem has a large range of possible keys so that it is not possible to just try all possible keys.

The security of a cryptosystem usually depends on the secrecy of the keys rather than the secrecy of the algorithm.

Keeping keys secret is one of the most difficult problems in practical cryptography. The keys typically have some mathematical structure, such as being the product of two large prime numbers.

The two most common types of cryptosystems are "symmetric-key" and "asymmetric-key" systems.

In symmetric-key cryptography, a message is encrypted and decrypted using the same key, as in the above story.

The key has to be passed along from one party to another in a separate transmission. A more secure method is asymmetric-key cryptography which is also known as "public-key" cryptography. This is based on using a pair of different keys (one "public-key" and one "private-key"). So each person now has two keys, one public-key that may be known to all, and one private-key that is known only to that person. These keys are related to each other in such a way that any message encrypted with the public-key can only be decrypted with the private-key and vice-versa. For example, if Jupe wants to send a secret message to Pete, he encrypts the message using Pete's public-key.

When Pete receives the encrypted message, he decrypts it using his private-key, to recover the original message.

The keys are designed so that finding out the private-key is difficult or impossible, even when the corresponding public-key is known.

Cryptography has a lot of application in computer networking. For example, it is used in online banking to maintain the confidentiality of any information being exchanged between you and the bank. It is also used to keep your password secure when you log into your email server. In general, any internet activity involving a financial transaction or requiring confidential information, depends upon a cryptosystem to keep the information secure during transmission.

While this may sound simple, a lot of intricacies have to be taken care of to ensure that the system work correctly.

For example, How can two computers exchange a secret key in public? How does the receiver detect if someone tampers with the information? How do the sender and receiver confirm each other's identity?

Figure 2: Redraw or edit attached gif image.

Box Information:

DES: The Data Encryption Standard (DES) cryptosystem is the most commonly used symmetric-key cryptosystem.
It was developed in 1977 by IBM.

RSA: RSA is the most commonly used asymmetric-key cryptosystem. It was developed in 1977 and is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.

Some interesting related websites are:
http://www.threeinvestigators.net/QM.html
http://www.cryptoclub.math.uic.edu/
http://www.42explore2.com/codes.htm
http://www.ssh.com/support/cryptography/introduction/

Illustrations: Mrs. Kaumudi Sahasrabudhe