PODCAST 3 - CRYPTOGRAPHY

MIKE ZABROCKI

Hi, my name is Mike Zabrocki and welcome to my third podcast for Math 2590.

Today I am going to explain to you a little about the main mathematical ideas behind cryptography.

When we send sensitive information over insecure channels (like the internet) we have some expectation of privacy, but networks of communication channels are public and therefore accessible to any thief with the right computer equipment.

Most of the time I'm quite trusting that no one wants to read that long rambling email that I sent to a friend of mine about my last vacation, but sometimes I want to send something private or, at the very least, not something I want everyone to have access to.

The best example of this is my bank password or credit card information which is potentially valuable to a thief.

When I sent my credit card number to a business, then I don't want some hacker collecting that card number and selling it to the highest bidder.

Similarly, when I log into my email account, I don't want just anyone to be able to read my email because I have a lot of sensitive information archived there.

Banks, businesses and governments have a much stronger need for making sure that information sent over communication channels is not intercepted and (potentially) changed.

The main way that information is kept secret when it is sent over insecure channels is that it is scrambled before it is sent and then unscrambled when the information is received at the other end.

The process of scrambling is called "encryption," and the process of descrambling the information is called "decryption."

If everyone knows how the encryption is done then there is no reason why the person listening in, say a spy or a thief, can't also decrypt the message.

To keep the process secret, part of the encryption and decryption is known only to the sender and the receiver (and hopefully not to the interceptor).

This secret part of the encryption and decryption is called the 'key.'

Encryption and decryption is usually a mathematical transformation on the message and the key is just a number which is used in the encryption transformation.

Many analogies with a physical key make sense in this context, it locks the message from someone who wishes to steal it.

As long as a key is changed frequently and only the sender and receiver have access to it, there is very little that an interceptor can do to recover the message without that key.

In a classical cryptography model, the sender and receiver need to have a key exchanged in advance of wanting to communicate to each other.

As electronic communication became more common, it became a bigger challenge to make sure that parties had keys that they both knew and that no one else could access.

I mention a classical cryptography model because in the 1970's one new idea revolutionized cryptography.

For example, imagine in modern warfare a battleship in the middle of the Pacific owned by a government.

In order to communicate with it the government would need to fly a helicopter out to the ship and physically hand that battleship a set of keys that they were sure no one else had access to.

You might think that they could (in theory) encrypt a set of keys and then send those keys by radio to the battleship, but then again, there was a need for a secret method for sending keys.

This sounds like a slightly exaggerated scenario, but it is even more complicated when you imagine that two people who have never met (say, me and Amazon.com) wish to communicate over a public communication network in a way that no one can intercept and potentially change a credit card transaction.

How do we exchange a key?

This was a difficult puzzle, but then in the 1970's, something changed.

Martin Hellman came up with a beautiful idea that he worked together with Whitfield Diffie to formulate.

Their abstract idea was to base security on the fact that some calculations are easy to do quickly, but the reverse calculation is hard to undo quickly.

If the calculation is large enough, it can take seconds to do, but thousands of years to undo.

This type of calculation is sometimes called a trapdoor function.

Their abstract idea was first put into practice by three mathematicians at MIT in the 1970's, Ron Rivist, Adi Shamir, and Leanord Adleman.

Their encryption scheme came to be known as RSA for their initials.

They devised an encryption scheme that bases security on the fact that it takes seconds for a computer to multiply a couple of hundred digit numbers together, but our current best algorithms take thousands of years to factor those numbers.

The system is ingeniously simple and uses theorems about integers that had been known for hundreds of years, but used in this way is simply brilliant.

Shortly after RSA was invented Whit Diffie and Martin Hellman came up with their own implementation of their another simple encryption scheme.

Their scheme bases security on the idea that it takes seconds to raise a number to a power with modular arithmetic, but thousands of years to figure out what power was used.

One remarkable property of these encryption schemes is that they base security on the fact that 'we think it is difficult to do a certain type of calculations.'

Tomorrow someone can come up with a clever way to factor integers or reverse raising to a power and the end result is that RSA and Diffie-Hellman key exchange will no longer be secure.

This desire to unlock secrets is a driving motivation for researchers to build faster computers and develop new mathematics.

Reference:
Steven Levy, Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age, Penguin (2002)