ED UW ZE FD SA IX (Cryptography)

Robert Hurley, Michael Mina, William Ivancic, Matthew Stewart   Advisor: Dr. Luiz Martins

Cryptography is the study of encoding messages so they are unreadable by those for which they were not meant. We will give a history of how the methods to do this have improved to meet with improved codebreaking.

Porta's digraphic cipher (1563)- A key (code word) smaller than the plaintext is decided on. Let's say our code word is CAB. The plaintext is then encrypted using that code word. We'll use the plaintext (X_p) BED. The ciphertext (X_c) is created by finding the intersection of the respective plaintext letter from the plaintext column, labelled X_p (in this case, the letter is B) and the respective ciphertext letter from the ciphertext column, labelled X_c, according to the "code word" (in this case, the letter is C). See Figure 1. This yields the first ciphertext character D. Using the same procedure for the second letter yields the ciphertext character E. The third ciphertext character also happens to be E. The completed ciphertext is DEE.

X_p	X_c		
A	A	B	C
B	B	C	D
C	C	D	E
D	D	E	F
E	E	F	G

Figure 1 (Porta's digraphic cipher). Xp: BED. Code word: CAB.

Playfair Cipher (1854): First both parties must agree to a password of moderate length. For this example, a very insecure password of "password" has been chosen. A 5x5 grid is filled, first left to right and then top to bottom, using each letter of the password that hasn't yet been used, then going in order of the alphabet, again omitting letters that have already been used. Another letter, in this case J, is also not in the table, since the table can only fit 25/26 letters, and j is not often used. It can commonly be assumed that j=i if it needs to be used, with that fact being obvious when the message doesn't completely make sense after decoding. See Figure 2.

The message we will be encoding is "go outside at noon." The message is broken into segments of two, also known as digraphs: go ou ts id ea tn oo n.

P	A	S	W	O
R	D	B	C	E
F	G	H	I	K
L	M	N	Q	T
U	V	X	Y	Z

Figure 2 (Playfair Cipher). Password: "Password"

With the rules we will soon discuss, two of the same letter in a group cannot be allowed, so an x is injected between them. If the number of letters was odd, another x would be tacked onto the end: go ou ts id ea tn ox on. Now to finally encode the message we use the following rules and our 5x5 table:

-If the two letters occupy the same row, replace them with the letters directly to their right

-If the two letters occupy the same column, replace them with the letters directly below them

-If the two letters occupy neither the same row nor column, complete the rectangle to which these two letters are two of the corners. The letters are replaced with the other two letters that make the corners of the rectangle, starting with the letter in the same row as the first letter being encoded. Doing this for each digraph yields: ka pz no gc do lq sz st. While during its original time of usage, this scrambled mess would be practically indecipherable, using modern technology it is solvable in seconds.

Cryptography was a key part of **World War II** strategy. The ability to intercept and decode secret messages was widely sought after by all sides in the war.

The **Enigma Machine (1920)** used by Nazi Germany to encipher and decipher messages involved the use of electrical currents and mechanical rotors to keep their secret messages safe.

Alan Turing was a British Mathematician who was able to break the Enigma cipher. This provided the Allied powers with access to Axis power communications that were enciphered with Enigma Machines. The military intelligence gained through the decryption of enemy communications was given the codename *Ultra*.

Time to break using modern technology	
Porta's	Under 1 second
Playfair	A few seconds
Enigma	Minutes
RSA	Years
Hashing	Not feasible

The **Diffie-Hellman Key Exchange (1976)** is a process by which parties can agree on a secret code using public data media without it being known by even someone intercepting all messages. While modern techniques to agree on this secret key are too complex to go into here, the basics of this practice can be explained more simply:

-Parties A and B agree on an entity, X, to start

-Both parties perform a secret operation on X, resulting in X_A for party A and X_B for party B

- X_A and X_B are exchanged between parties A & B

-Both parties perform the same operation they did before on their new entity leaving party A with X_{BA} and party B with X_{AB}

-The operations are chosen in a specific way such that X_{BA} = X_{AB} and a secret key is shared

In order to understand how **RSA works**, we must first understand some foundational topics.

RSA Cryptography (1973) works in the following way: First, two distinct primes, p, q, are selected. Next, compute $m = pq$ and $\phi(m) = (p-1)(q-1)$. A random d is selected such that $gcd(d, \phi(m)) = 1$. Then $e = d^{-1} mod\ \phi(m)$ is computed. Lastly, e and m are published.

In order to encrypt, the following formula is used: $X_c = X_p^e\ mod\ m$, where X_c is the ciphertext, X_p is the plaintext. Conversely, decryption follows the formula $X_p = X_c^d\ mod\ m$.

Cryptographic Hashing (~1995) is a method of taking the value of an input into a hashing function to receive a unique fix-width value, usually a hexadecimal string, sometimes called a checksum or a digest. The basic principles of a cryptographic function are ease of calculability, difficulty of recreation, and unlikelihood of similarity. The basic idea of a hash function is to take a large amount of input and create a small amount of output that uniquely identifies the input. The most commonly used cryptographic functions are SHA-1 and MD5. Some applications of cryptographic hashing are ensuring data integrity during delivery and password checking. For example, the receiver knows the hash value of a given set of data but not the actual set of data, can verify with the sent hash value that it is the same.