Encryption Codes for Family Safety

Joseph Parish

I have recently been reviewing all that I know about the “One-time pad” as used in decryption. This was a popular method employed by NSA, and assigned a code name of “DIANA”. There was a general-purpose pad designed with codenames “CALYPSO”, “ORION”, “MEDEA”, and “MICKEY MOUSE” as well. There were several automatic systems that were specially created by the NSA for the CIA, and Special Forces units. To provide a quick overview of the One Time Pad, it is an encryption technique which generally cannot be cracked, however, it does require a one-time pre-shared key. With this technique, a plain text is paired with a random secret key where each character of the plaintext is encrypted by simply combining it with the corresponding character from the pad. This system was popular with both NSA, and the Russian KBG. Naturally, like in any spy drama the paper that the pads used was highly flammable, and could readily be disposed of after use. Even NSA, and KBG cannot decipher the message without the proper pad being used.

I am not going to go into a lot of detail here, but I merely wanted to mention this in case anyone wanted to develop a similar structure for their own family. The process would actually be fairly simple to accomplish. Although not exactly like the One Time Pad, it will function successfully. Take a book, and it can be any book you wish to use. As an example, you might decide to use a bible. The key is to make sure that you, and the person you are sending the code to are using the exact same book including the edition. They should be mirror copies of each other. You will never mention the book again.

You know exactly what book you are deciphering the code from so suppose someone sends you a code as follows:

45-5-6

90-12-4

30-1-8

160-41-6

22-10-5

Suppose you and your friend are using a certain bible to get your codes deciphered. You would first turn to page 45. Next go down the page to line 5. Finally work your way across to the 6th letter. As an example, suppose the sixth letter is an “H” than that is your first letter.

Doing the same for the next letter you select page 90, and go to line number 12 and finally to letter number 4, and in our hypothetical code the letter is “I”. Continuing on we could decipher the remaining code as “JOE”. No spaces are given, and you would need to assume where the spaces will go as in this case it is “HI JOE”.

This system is only secured, and protected if no one knows what book you are using. The beauty of this system is that you can walk around with a bible in your hand, and no one would be the wiser. There are a number of modifications to this system that you could make to create a more secure process. You could start your count from the end of the book. If the code says ten and you have 350 pages you could go to page 340, and not to page 10 if going in reverse.

When I was in the military my wife, and I had a system setup where if I contacted her with a letter, I would enlarge certain letters within the correspondence. The rules state that capital letters at the beginning of a sentence do not count. I would only use those letters within the sentence, and they should be properly spaced so as to not draw attention to them. To read it, you simply list each of the letters and place spaces where they should logically be. The system will work, and should be practiced. I hope this information helps families to develop an emergency notification procedure.