Theoretical and Practical Significance of One-Time-Pad Cryptography

Luka Komljenovic, Jonathan Wright, Timothy Szeltner | David Aloi | Cleveland State University

1 Introduction

- Cryptography involves the encryption and decryption of coded messages using a key
- Some keys are generated based on a predictable algorithm, resulting in unintended decryption
- The One Time Pad (OTP) system uses a random key shared by sending and receiving parties to create a mathematically unbreakable code that reveals no information about the sent message

2 Theory

- OTP encryption uses completely random keys to successfully convey the message
- Every key must be the same length as the plaintext of the encrypted message, and have no pattern such as one produced by an algorithm
- Messages and keys may be in binary, decimal, or base 26 in the case of the alphabet, which are then added modularly with that base to produce the encrypted message

Limitations:

- Keys can only be used once
- Keys must be as long as the sent message
- Keys must be securely exchanged

3 Process

A(1)	**T(20)**	**T(20)**	**A(1)**	**C(3)**	**K(11)**	
D(4)	**D(4)**	**D(4)**	**D(4)**	**D(4)**	**D(4)**	**(+)**
E(5)	**X(24)**	**X(24)**	**E(5)**	**G(7)**	**O(15)**	

- This Caesar cipher example uses a shift of 4 for every character, where "**ATTACK**" becomes "**EXXEGO**"
- This is not very secure if it is known a Caesar cipher is being used, as there are only 26 possible messages to be coded.
- Consider a case where an OTP encrypted message is intercepted: "**JVMLQM**"

A(1)	**T(20)**	**T(20)**	**A(1)**	**C(3)**	**K(11)**	
I(9)	**B(2)**	**S(19)**	**K(11)**	**N(14)**	**B(2)**	**(+)**
J(10)	**V(22)**	**M(13)**	**L(12)**	**Q(17)**	**M(13)**	

- Using a key of "**IBSKNB**", the message can be decrypted as the word "**ATTACK**"

R(18)	**E(5)**	**T(20)**	**U(21)**	**R(18)**	**N(14)**	
R(18)	**Q(17)**	**S(19)**	**Q(17)**	**Y(25)**	**A(1)**	**(+)**
J(10)	**V(22)**	**M(13)**	**L(12)**	**Q(17)**	**M(13)**	

- Using an equally valid key of "**RQSQYA**" can produce the decrypted contradictory message of "**RETURN**"
- The difficulty of decryption increases exponentially because each character has a random shift associated with it, that can produce equally valid decrypted messages
- There are 26^5 possible messages associated with the encrypted phrase "**JVMLQM**", or 26^N for a message of length N

4 Application

- Many countries' intelligence services have used OTP Cryptography to send messages among its agents in secrecy because of its unbreakable nature, including Germany, the US, and USSR since the early 1900's
- Modern "numbers stations" broadcast alphanumeric messages over public frequencies to military assets without fear of decryption, such as the US Emergency Action Messages, or SKYKING broadcasts
- The US-USSR hotline was actually an OTP encrypted teletype machine using a XOR operation that transmitted written messages to avoid the inconsistencies and security risks of using voice messages and interpreters.

5 Conclusion

- OTP has its place where the secrecy of the message is paramount, and secure exchange of keys is guaranteed
- The drawbacks of large key length and transmission of the key between parties limits the applications of OTPs, especially in modern computer systems

6 Works Cited

1. Rijmenants, D. (2016). *THE COMPLETE GUIDE TO SECURE COMMUNICATIONS WITH THE ONE TIME PAD CIPHER* (4th ed., Vol. 7, pp. 1-27, Rep.).
2. *Shannon, Claude (1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal.* ***28*** *(4): 656–715.*
3. One Time Pad. (2012, August 13). Retrieved April 4, 2017, from http://cryptomuseum.com/crypto/otp/index.htm