Assignment 1
Brute Force Attack Estimation

L. Towell,
Student No: 201383538

December 3, 2019

Code repository: COMP522-Assignment 2

1 Comparison of methods for message authentication

1.1 Hash-functions

1.1.1

1.2 RSA + SHA1 method

1.3 DSA method

1.4 HMAC-SHA256 method

2 Diffie-Hellman with 4 parties

2.1 Design for the Diffie-Hellman Protocol

Following the principles of the Diffie Hellman Protocol means that in order to read the messages that are being transmitted every party needs to know the public key of all of the other members in the network in order to generate a shared secret key.

The process is largely the same when more parties are added however because more parties have been added it means that more keys need to be generated and shared. Each party starts the process by using the shared prime number (q) and the shared primitive root (α of q)

Each key then generates their public keys using an random integer that they have generated.
$Y_A = \alpha^{X_A}$ mod q
$Y_B = \alpha^{X_B}$ mod q
$Y_C = \alpha^{X_C}$ mod q
$Y_D = \alpha^{X_D}$ mod q

The above keys are then shared among all members of the network then the following calculations are performed in order to calculate the secret Keys
A calculates K = $(Y_{BCD})^{X_A}$ mod q
B calculates K = $(Y_{ACD})^{X_B}$ mod q
C calculates K = $(Y_{ABD})^{X_C}$ mod q
D calculates K = $(Y_{ABC})^{X_D}$ mod q

2.2 Implementation of the Protocol with 4 Parties

2.3 Conclusion

As can be seen from the code in *Appendix D.* I have had to exchange all of the keys amongst each of the members in the network. I have done this through multiple iterations (phases) of the network in order for everyone within the network to have all of the keys needed to successfully generate a shared secret key for

decoding messages that are sent. *figure 1.* shows the iteration cycle of how keys are exchanged over multiple iterations.

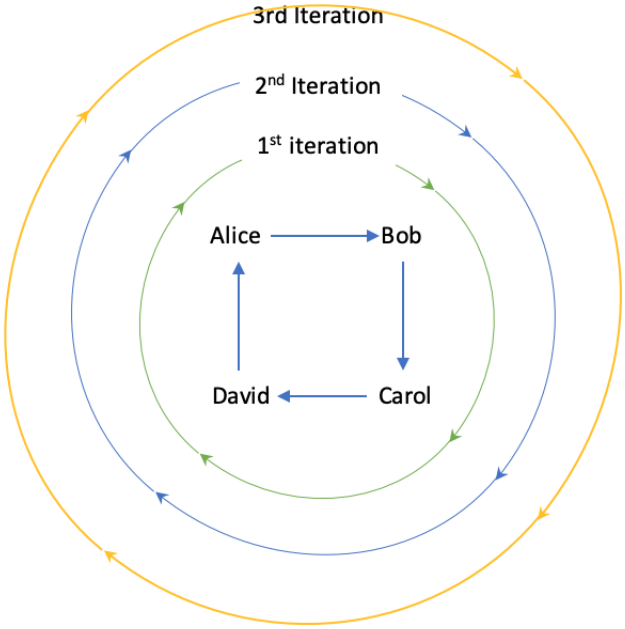

Figure 1: Diagram of how keys are passed between members of network.

Table 1. below details how the keys are gathered. In iteration 0 the only keys that each members have are their own however as we iterate around the network the keys are gathered until every member has every other members public keys which enables them to be able to decode the messages that have been encrypted with private keys.

	Public Keys held by network members			
N	Alice	Bob	Carol	David
0	A	B	C	D
1	AD	BA	CB	DC
2	ADC	BAD	CBA	DCB
3	ADCB	BADC	CBAD	DCBA