1. Key exchange refers to the sharing of an identical key between two parties. In the case of public / private key scenarios, the public key is shared between them. On the other hand, key agreement occurs when each party mixes their private key with their obtained public key, sends their mixtures to each other and then adds their private keys to the other’s mixture. This results in a shared key, used to both encrypt and decrypt the messages sent between them.
2. The discrete logarithm problem is the attempt to reverse a secret value in terms of its modular expression, by working out what the primitive root of a secret number has been raised to. The number it is raised to determines a new secret value each time that can be used to encrypt a message, so attempting to calculate this in reverse requires many trial-and-error operations.
3. In my opinion, given the early stages of investigation into how the internet works as well as the low computing processing power at the time, it would even take a long time to figure out the time it took to crack the messages that utilised this protocol. In addition, formulas like these require a lot of patience and trial-and-error in themselves to identify the method which works the best and is least likely to be cracked.
4. The one-way-function, highlighting how it can be easy to perform an operation (in this case encryption) in one direction, yet incredibly difficult to perform in reverse (in this case decryption).
5. The “logjam” attack can be performed, allowing an attacker to read and intercept any data passed over a network between the two parties sharing their encrypted message.
6. How many keys..

PrAlice

PrBob

PrMallory

PubAlice

PubBob

MixBob

MixAlice

SharedAliceBob

My guess is 8

1. No timestamps and provides [perfect forward secrecy](https://en.wikipedia.org/wiki/Perfect_forward_secrecy)
2. Too long..

p = 11

g = 2

Alice x = 4

Bob y = 3

Public z = 29

Alice