Thomas Hart

CS 465 HW #5

Diffie Hellman

The Diffie Hellman protocol has some public numbers 'g' and 'n'. Two different people (Alice and Bob), have a private key each, which are always prime numbers. Let's say Alice wants to send a message to Bob. Alice first gets Bob's public key, which is g^b modulus g^n. Alice then uses her own private key to further the calculation. The result will be (g^b mod g^n)^a mod g^n. She encrypts her message using this key. Next, Alice sends her message out, along with her public key to Bob. Her public key is g^a mod g^p. Bob will receive the ciphertext and combine his private key with Alice's public key. This will be (g^a)^b mod g^n. Because (g^a)^b and (g^b)^a are equivalent values, Alice can encrypt her message with the key, and Bob can decrypt the message with the same key.

The security here is that there are so many different possible prime numbers in the range of g^n, or p – the prime modulus. It is also near impossible to use the two public keys to determine what the exponent was to reach that key since the result is a modulus number. There are also other complexities with prime numbers that make an attack infeasible. This algorithm has been around a long time and is still considered secure.

Man in the Middle Attack

Because it is infeasible to discover a private key with this secure protocol, a man in the middle attack is necessary to eavesdrop or tamper with the messages. With a man in the middle attack, the attacker, Mallory, convinces Bob that she is actually Alice, and she convinces Alice that she is actually Bob. This way, the Diffie Hellman algorithm doesn't need to be broken. It's used by Mallory to act as the (wo)man in the middle, while Alice and Bob think it is just the two of them.

The attack happens during the exchanging of public keys. Mallory gives her own public key to Alice and another public key to Bob. Then Alice and Bob will willingly exchange their public keys with Mallory, which will allow her to read and tamper with the messages back and forth.

Prime Modulus P

What is the recommended key size for the prime modulus p in DH?

2048 bits

Why is the recommended size for p for DH so much larger than the recommended key size for AES?

In AES, the size of the of the key is a protection against a brute force attack. In a 128-bit key, a person must check 2^128 options in the worst case. That number is too high for any computer today to compute. With Diffie Hellman, the key range is much higher at 2^2048 bits. The number must be a product of two prime numbers, though, which significantly decreases the number of possibilities. This narrowing of options is why the range must be so wide.