Cryptographically Protected Telephone System

Adam Yedidia and Andres Erbsen

October 22, 2014

For our final project, we plan on making a telephone system that will be cryptographically protected. In other words, sounds made on one end of the telephone system will be audible on the other side of the telephone system, and it will be very difficult for an eavesdropper to recover the sounds transmitted over the telephone system, even when the eavesdropper is given access to a perfect wiretap, i.e. the composition of all signals sent through the system.

More precisely, our encryptions of sounds transmitted across the telephone system will be secure assuming that a polynomial-time algorithm for finding elliptic-curve discrete logarithms is not found. Our project will be based on the paper, "Curve 25519: new Diffie-Hellman speed records" by Daniel J. Bernstein; in his paper, Bernstein notes, "The general problem of elliptic-curve discrete logarithms has been attacked with very little success.... [it] is conjectured to be extremely difficult." The security of our telephone system will be based on the assumption that elliptic-curve discrete logarithms are indeed hard to find; we will use a prime groupe greater than 2^{252}, which is the size that Bernstein suggests to be safe from brute-force attacks.

Our cryptographic system, at a high level, will be based around the Diffie-Hellman scheme for encryptying information such that it will be indecipherable to an eavesdropper despite there being no prior agreements between the two communicating parties. In the standard Diffie-Hellman scheme, we assign to each person a private key (call them a and b). From those two private keys and some public values g and p, the two interlocutors compute their public keys, $g^a \bmod p$ and $g^b \bmod p$. To encrypt a message, both interlocutors can compute the shared secret $g^{ab} \bmod p$ from a combination of their private key and their colleague's public key; an eavesdropper, however, lacking access to either private key, cannot compute the shared secret. Finally, the message m is encrypted by computing the bitwise XOR of the message with the shared secret; the ciphertext c is given by the formula $c = m \oplus (g^{ab} \bmod p)$. In standard Diffie-Hellman, integer operations are used; we will use a more efficient implementations which generalizes the notions of multiplication and exponentiation to elliptic curves (another realm where multiplication and exponentiation are easy but logarithms are hard.)

Aside from the security aspect, the goal of this project will be to faithfully transmit sound across a channel.