ElGamal and Diffie-Hellman

G. Averkov
Brandenburg University of Technology

May 24, 2024

Alice chooses an element g of a multi-digit order n in a group $(G, \cdot)$ and fixes $k \in \{2, \ldots, n-2\}$ as her private key. She makes n, g, g^k public.

Alice chooses an element g of a multi-digit order n in a group $(G, \cdot)$ and fixes $k \in \{2, \ldots, n-2\}$ as her private key. She makes n, g, g^k public.

To send $x \in G$ to Alice, Bob generates a random $t \in \{2, \ldots, n-2\}$ and sends the pair $y = (y_1, y_2)$ with $y_1 = g^t$ and $y_2 = x(g^k)^t = xg^{kt}$ as a cipher text.

Alice chooses an element g of a multi-digit order n in a group $(G, \cdot)$ and fixes $k \in \{2, \ldots, n-2\}$ as her private key. She makes n, g, g^k public.

To send $x \in G$ to Alice, Bob generates a random $t \in \{2, \ldots, n-2\}$ and sends the pair $y = (y_1, y_2)$ with $y_1 = g^t$ and $y_2 = x(g^k)^t = xg^{kt}$ as a cipher text.

Alice, deciphers by calculating $y_2 y_1^{-k} = xg^{kt}(g^t)^{-k} = x$.

In order to break the cryptosystem, Eve needs to solve the discrete logarithm problem (DLP), by determining k from the knowledge of n, g, g^k.

In order to break the cryptosystem, Eve needs to solve the discrete logarithm problem (DLP), by determining k from the knowledge of n, g, g^k.

In order, to break the cipher, Eve needs to solve the system $g^t = y_1, x(g^k)^t = y_2$ in the unknown t and x. Determination of t requires solving the DLP, too. Once t is determined, one gets the plain text $x = y_1 y_2^{-t}$.

In order to break the cryptosystem, Eve needs to solve the discrete logarithm problem (DLP), by determining k from the knowledge of n, g, g^k.

In order, to break the cipher, Eve needs to solve the system $g^t = y_1, x(g^k)^t = y_2$ in the unknown t and x. Determination of t requires solving the DLP, too. Once t is determined, one gets the plain text $x = y_1 y_2^{-t}$.

ElGamal encryption is used on groups, where no efficient methods of solving DLP are known.

Diffie-Hellman key exchange

Alice and Bob want to generate shared private data (so called shared secret). For example, they can use it as a shared key in symmetric cryptosystems. However, they can only communicate over the public domain. What they can do is this. They establish two copies of ElGamal, one for Alice and one for Bob, that are based on the common $g \in G$ in the group $(G, \cdot)$. That means, Alice fixes her private key $a \in \{2, \ldots, n-2\}$ and publishes g^a, while Bob fixes his private key $b \in \{2, \ldots, n-2\}$ and publishes g^b. Now, Alice raises Bob's g^b to the power a, and Bob raises Alice's g^a to the power b. This way Alice and Bob have the shared secret $g^{ab} = (g^a)^b = (g^b)^a$, even though the could not meet privately and have been communicating exclusively through the public domain.

	Alice's private area	Public domain	Bob's private area
Step 1		$g \in G$	
Step 2	a	g^a $\quad$ g^b	b
Step 3	$g^{ab} = (g^b)^a$		$g^{ab} = (g^a)^b$

The public domain contains g^a and g^b. There seem to be no direct ways to get g^{ab} out of g^a and g^b. Eve could take powers of g^a and g^b and multiply them obtaining $(g^a)^i(g^b)^j = g^{ia+jb}$, but it is not clear which of these powers (if any) is equal to g^{ab}. So, there seems to be no other way than obtaining a and b by solving two instances of the DLP, then calculating ab and raising g to the power ab to obtain g^{ab}. If Eve does not know any efficient ways to solve the DLP in the group $(G, \cdot)$, she will have hard time to proceed in this way.