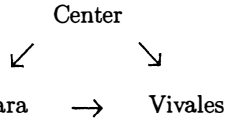
Notice that Pícara can easily check that $\beta_1\beta_2 = C$, and thus be sure that Vivales does not know the discrete logs of both elements of his public key (β_1, β_2). Since it is in Vivales' interest to get as much information as possible, Pícara can be sure that he does know the discrete log of one of the two elements. But there is no way Pícara can distinguish between β_1 and β_2 for the purpose of determining which Vivales obtained as b^x and which as C/b^x. Thus, both Vivales and Pícara can be confident that the above conditions (1) and (2) are fulfilled.

If a sequence of pairs (m_1, m_2) are sent using the same (β_1, β_2) (i.e., the same values of x and i), then Pícara does know that the element of the pair (m_1, m_2) that Vivales is deciphering (namely, m_i) remains the same for all pairs of message units in the sequence. If we want another sequence of message units to be sent independently, then Vivales must randomly select new values for x and i, and send a new public key (β_1, β_2).

Use of oblivious transfer for a non-interactive proof of factorization. The idea conveyed by the term "non-interactive" can be summarized in the form of a diagram



Here the "trusted Center" can be thought of as a source of random bits, which are sent simultaneously to Pícara and Vivales (it is permissible for the Center first to perform some arithmetic operations on the bits before sending them). The combination of these bits and Pícara's reaction to them — what she sends Vivales — must be enough to convince Vivales (with an exponentially decreasing chance that he's being fooled) that she did what she claims to have done.

The "non-interaction" means that in the course of the proof Vivales does not communicate to Pícara. However, it is permitted that at the very beginning Pícara has been given a long sequence of oblivious transfer public keys (β_1, β_2) for Vivales, as described above. This is not counted as a communication from Vivales to Pícara. In fact, the same public keys are available, as the word "public" suggests, for anyone to use who's playing the role of Pícara. And Pícara can use the same sequence of public keys in many different zero-knowledge proofs she sends to Vivales.

We now describe the procedure that Pícara uses to convince Vivales that she can factor an integer $n = pq$ without giving him any information about what its factors might be. We will use the fact that the ability to take the square root modulo $n = pq$ of an arbitrary number that has a square root is equivalent to knowledge of p and q (see Exercise 5 below). The procedure is as follows:

1. The Center randomly generates an integer x, and sends Pícara and Vivales the least nonnegative residue of x^2 modulo n; let us denote $y = x^2 \bmod n$.