Aïda knows bB (which is public knowledge) and her own secret a. However, a third party knows only aB and bB. Without solving the discrete logarithm problem — finding a knowing B and aB (or finding b knowing B and bB) — there seems to be no way to compute abB knowing only aB and bB.

Analog of Massey–Omura. As in the finite–field situation, this is a public key cryptosystem for transmitting message units m, which we now suppose have been imbedded as points P_m on some fixed (and publicly known) elliptic curve E over $\mathbf{F}_q$ (where q is large). We also suppose that the number N of points on E has been computed (and is also publicly known). Each user of the system secretly selects a random integer e between 1 and N such that $g.c.d.(e, N) = 1$ and, using the Euclidean algorithm, computes its inverse $d = e^{-1}\ mod\ N$, i.e., an integer d such that $de \equiv 1\ mod\ N$. If Alice wants to send the message P_m to Bob, first she sends him the point $e_A P_m$ (where the subscript A denotes the user Alice). This means nothing to Bob, who, knowing neither d_A nor e_A, cannot recover P_m. But, without attempting to make sense of this point, he multiplies it by *his* e_B, and sends $e_B e_A P_m$ back to Alice. The third step is for Alice to unravel the message part of the way by multiplying the point $e_B e_A P_m$ by d_A. Since $NP_m = O$ and $d_A e_A \equiv 1\ mod\ N$, this gives the point $e_B P_m$, which Alice returns to Bob, who can read the message by multiplying the point $e_B P_m$ by d_B.

Notice that an eavesdropper would know $e_A P_m$, $e_B e_A P_m$ and $e_B P_m$. If (s)he could solve the discrete log problem on E, (s)he could determine e_B from the first two points and then compute $d_B = e_B^{-1}\ mod\ N$ and $P_m = d_B(e_B P_m)$.

Analog of ElGamal. This is another public key cryptosystem for transmitting messages P_m. As in the key exchange system above, we start with a fixed publicly known finite field $\mathbf{F}_q$, elliptic curve E defined over it, and base point $B \in E$. (We do not need to know the number of points N.) Each user chooses a random integer a, which is kept secret, and computes and publishes the point aB.

To send a message P_m to Björn, Aniuta chooses a random integer k and sends the pair of points $(kB,\ P_m + k(a_B B))$ (where $a_B B$ is Björn's public key). To read the message, Björn multiplies the first point in the pair by his secret a_B and subtracts the result from the second point:

$$P_m + k(a_B B) - a_B(kB) = P_m.$$

Thus, Aniuta sends a disguised P_m along with a "clue" kB which is enough to remove the "mask" $ka_B B$ if one knows the secret integer a_B. An eavesdropper who can solve the discrete log problem on E can, of course, determine a_B from the publicly known information B and $a_B B$.

The choice of curve and point. There are various ways of choosing an elliptic curve and (in the Diffie–Hellman and ElGamal set-up) a point B on it.

Random selection of (E, B). Once we choose our large finite field $\mathbf{F}_q$, we can choose both E and $B = (x, y) \in E$ at the same time as follows. (We