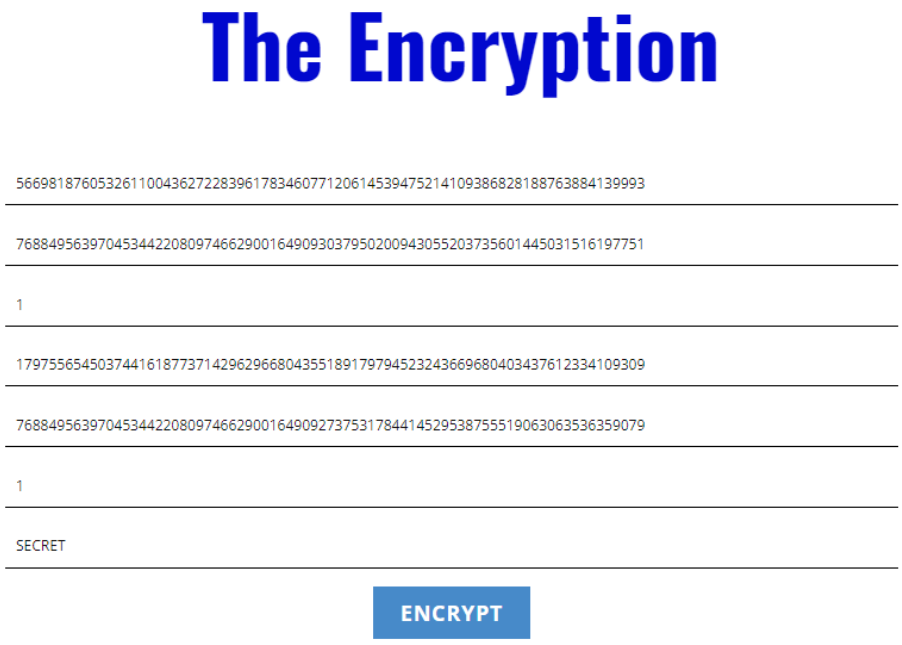
The figure below is the web page for entering the values for the domain parameters of the cryptosystem.

here the curve with key size 256-bit is used and the message to be encrypted is "secret".



The following figures display an encryption and decryption experiment and shows the cryptosystems phases in this order: the keys generation, the message encoding, the encryption, to decryption and finally the decoding.

Keys Generation

in this phase each user selects a random integer as its private keys in this phase and then computes its public keys using the following methods.

Alice private key is ?
27361679287871322366130720056640629860847291260089887871467579726043946045507.
Bob private key is
20070926947659122713621450838348885774677326230629618698238356023970673775801.
Alice public key is
(47183305756158899809209459583003308878176043840611396822768574412291329028534
,27007327663009293735215813812577171289952667121066371931982985854063357733660,0).
Bob public key is
(45591242898457960807800228289238918938294429438969684782456160609998168478055
,52810052456296855273212864662319037226807874563312430998602461902352542680280,0).

Message Encoding

In the message encoding phase, each char in the message is mapped to its corresponding point in the lookup table that the two entities agree upon.

The message mapped points are
(104,546310592264911188575959441544034666701160971595783371358801735293051396552 56,1)
(91,178045756901912733327288023966199575641027995947068050334194501896034108358 21,1)
(89,359131077736596127205152512156633398649064351567582506807055690089024970670 00,1)
(104,222538971705542253632138024745981824229218530413647180678554279157263765424 95,1)
(91,178045756901912733327288023966199575641027995947068050334194501896034108358 21,1)
(105,481186170187548736770918570773258721694898215498319786004182153359436434334 47,1)
(26,670384532339642302564705728071405527634598013557083524376404709221383937169 05,1).

Encryption

In this phase, the cryptosystem will encrypt the point array representing the message after encoding to produce a cipher array.

The message cipher points are
(373872054155950117239391508008348461787691308878147540072769775775825626506 65,3056177446804359461408896095682687863039665304432831117871620905887460779 3593,0)
(447539803751808375780477898075756585905387006768573720858654067996733654930 51,6717214396669430541916352288885521215066966962821617938521038805342462822 1969,0)
(741641230518113932174000404308324820485776004243785621519668157374157802926 69,20555961972308945551379063675750625730412443709167772198538361231444531953 320,0)
(286534134551355231070736774989402027840180632623469473235793023663973613830 17,3067306933692949131277905749263489239919727847343194897651372524856812633 5827,0)
(447539803751808375780477898075756585905387006768573720858654067996733654930 51,6717214396669430541916352288885521215066966962821617938521038805342462822 1969,0)
(157724325403836183270468400985522354285365637268014868652511789288319450590 99,4855137527686412811287080636226972557663763419641223305817627329382060804 3273,0)
(116284651983322495515247518906476447844603398010292444401859256153065797827 26,6934370139749519826922150977480417963511468357034494332136257847385893762 5276,0).

Decryption

In this phase, the cryptosystem will decrypt the cipher points.

The m?essage decipher points
are (104,546310592264911188575959441544034666701160971595783371358801735293051 39655256,0)
(91,178045756901912733327288023966199575641027995947068050334194501896034108 35821,0)
(89,359131077736596127205152512156633398649064351567582506807055690089024970 67000,0)
(104,222538971705542253632138024745981824229218530413647180678554279157263765 42495,0)
(91,178045756901912733327288023966199575641027995947068050334194501896034108 35821,0)
(105,481186170187548736770918570773258721694898215498319786004182153359436434 33447,0)
(26,670384532339642302564705728071405527634598013557083524376404709221383937 16905,0).

Message Decoding

In the message decoding phase, each EC point i is mapped back to its corresponding char in the lookup table that the two entities agree upon.

The message is secret