*Function* fixed\_hash

*Input Arguments*

* X1, x2 – are two binary strings
* The function internally uses P the prime, G, H are the two generators of the prime
* n- is the length of the prime P in binary bits

*Output*

* Hash value - A binary string

*Logic*

* This function internally uses Discrete Logarithm function
* Res1 is the output of DL with G, x1, P
* Res2 is the output of DL with H, x2, P
* The final result is product of res1 and res2 under modulo of P
* The result is covert to binary string and then prepended with zeros till the length is n (length of P in binary)

*Usage*

This function is used in var\_hash (Merkle Damgard) which is then used in HMAC