

To scramble: select r randomly from $\{1 \dots q\}$ and calculate $g' = g^r$ and $h' = h^r = g^{xr}$.

```
Function encrypt( $G, g', q, h', m$ ) {  
  select  $y$  randomly from  $\{1 \dots q\}$   
   $c_1 = g'^y$   
   $s = h'^y$   
   $m' = m$  converted to a member of  $G$   
   $c_2 = m' \cdot s = m' \cdot h'^y = m' \cdot g^{xry}$   
  return  $(c_1, c_2)$   
}
```

```
Function decrypt( $G, x, c_1, c_2$ ) {  
   $s = (c_1)^x$   
   $m' = c_2 \cdot s^{-1} = m' \cdot g^{xry} \cdot g^{-xry}$   
   $m = m'$  de-converted from a member of  $G$   
  return  $m$   
}
```