

Example of signature realization with Octave

Public Parameters generation: **PP** = (**p**, **g**)

p - is strong prime if
 $p = 2 * q + 1$, when q - is prime.
 Then $q = (p-1)/2$

```
>> p= int64(268435019)
p = 268435019
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 134217509
>> isprime(q)
ans = 1
>>
>> pb=dec2bin(p)
pb = 1111 1111 1111 1111 1110 0100 1011
      F   F   F   F   E   8   B
```

```
>> p=genstrongprime(28)
p = 201108443
>> q=(p-1)/2
q = 100554221
>> isprime(q)
ans = 1 % p is a strong prime
>>
>> g=2
g = 2
>> mod_exp(g,q,p)
ans = 201108442 % not equal to 1
>> mod_exp(g,2,p) % not equal to 1
ans = 4 % the generator is g=2
```

```
>> x=int64(randi(p-1))
x = 155678120
>> a=mod_exp(g,x,p)
a = 151170722
```

```
>> m='Hello Bob'
m = Hello Bob
>> u=int64(randi(p-1))
u = 228451192
>> r=mod_exp(g,u,p)
★ r = 186468078
```

```
>> cc=concat(m,r)
cc = Hello Bob186468078 % cc is a string type variable
>> cc=concat(m,'33418907')
cc = Hello Bob33418907
>> ccc=concat(m,'r')
ccc = Hello Bobr
```

```
>> h=hd28(cc)
h = 25029435
>> s=mod((u+x*h),p-1)
```

```
>> g_s=mod_exp(g,s,p)
g_s = 6360091
V1=g_s;
>> a_h=mod_exp(a,h,p)
a_h = 9793036
>> V2=mod(r*a_h,p)
V2 = 6360091
```

$h = 25029435$

$\gg s = \text{mod}((u+x \cdot h), p-1)$

$s = 22064560$

