

Mini-https

Confidential, Integral, Authentic

Public Parameters $PP = (p, g)$.
 $p = 268435019$; $g = 2$;



$(E, D), (Sign, Ver)$
 Hand shaking PuK_A



$PrK_B = y = \text{randi}(p-1)$
 $PuK_B = b = g^y \text{ mod } p$

$PrK_A = x = \text{randi}(p-1)$

$PuK_A = a = g^x \text{ mod } p$

AKAP

$G, \sigma = (r, s)$

$PuK_A = a$

k

$E(k, T) = C$

Encrypt & sign paradigm

Chosen ciphertext security

CCS

$h_c = H(C)$

$Sign(Prk=x, h_c) = \sigma = (r, s)$

By realizing Schnorr - sign

$i \leftarrow \text{randi}(p-1)$

$r = g^i \text{ mod } p$

$h_c = H(C || r)$

$s = (i + x \cdot h_c) \text{ mod } p$

1. $Ver(PuK_A=a, \sigma) = \{T, F\}$
2. $D(k, C) = T$
3. Performs money transf.



MINI-HTTPS
 €5.00

1. Mentor sends you Public Parameters ($p = 15728303$; $g = 5$) of 24 bits length. Generate public and private keys $PrK_A = x$ and $PuK_A = a$. Send public key a to the Mentor.

12677229

```
>> p=int64(15728303)
p = 15728303
>> g=5;
>> x=int64(randi(p-1))
x = 9712179
>> a=mod_exp(g,x,p)
a = 12677229
```


Success! You have finished the task. Great job!

Get reward