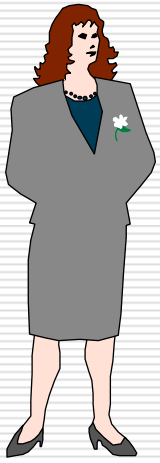
Diffie-Hellmann

Slightly simplified ...

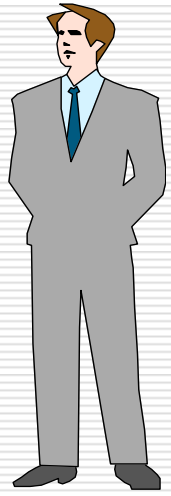
Alice



Hi Bob,
We need to talk.
Confidentially!

Hi Alice,
We need to talk.
Confidentially!

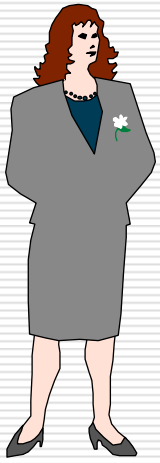
Bob



Sorry, no
chance ...

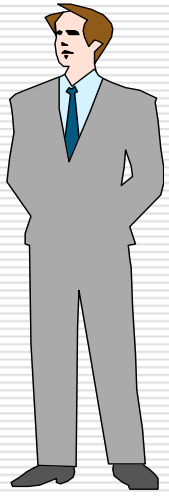
Mallory

Alice



First, we need a big prime number.

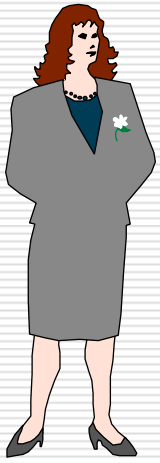
Bob



useless, I'll get you!

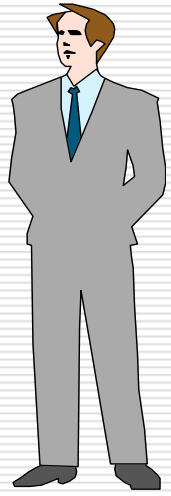
Mallory

Alice



Lets take **n=13**.

Bob



n=13

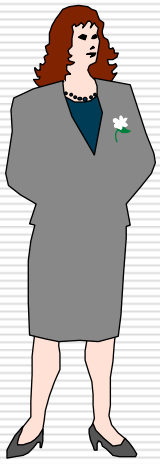
n=13

Now I know the number **n**!

Mallory

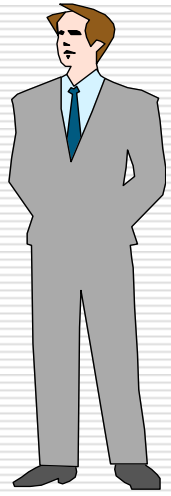
n=13

Alice



Oh Bob, your **n** is so huge ...

Bob



n=13

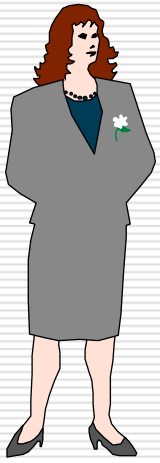
n=13

Now I know the number **n**!

Mallory

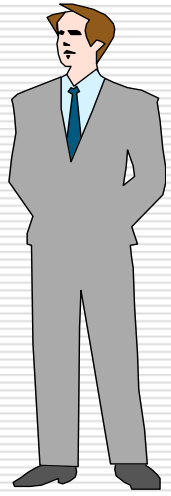
n=13

Alice



Aditionally we need a random number.

Bob



n=13

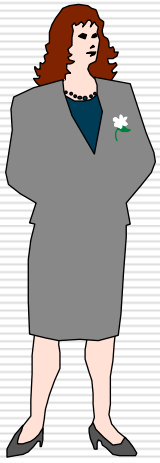
n=13

useless, I'll get you!

Mallory

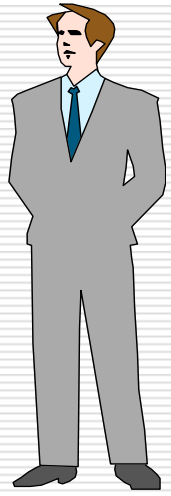
n=13

Alice



by chance i got the number **g=6.**

Bob



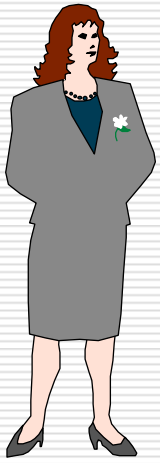
n=13
g=6

Now I also have the number **g**!

Mallory

n=13
g=6

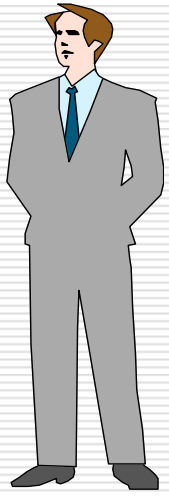
Alice



n=13
g=6

Great!

Bob



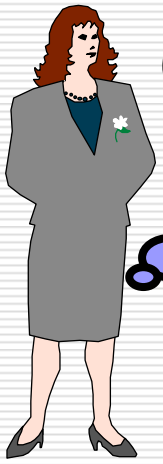
n=13
g=6

useless, I'll get you!

Mallory

n=13
g=6

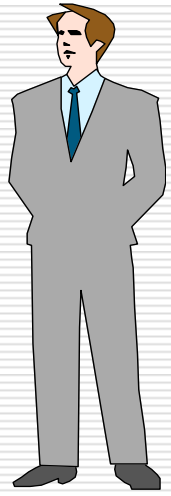
Alice



My private random number is: **x=5**

My private random number is: **y=7**

Bob



n=13
g=6
x=5

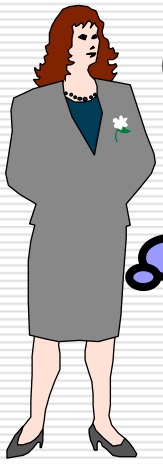
What the hell are they doing now?

Mallory

n=13
g=6

n=13
g=6
y=7

Alice

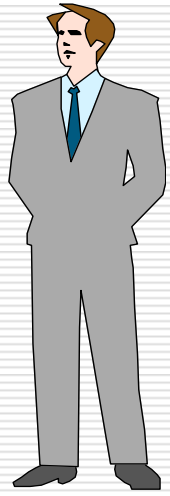


Now I calculate my public number:

n=13
g=6
x=5

Now I calculate my public number:

Bob

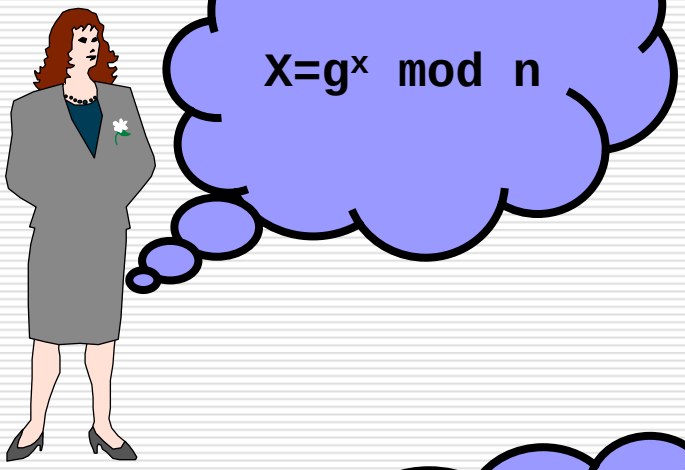


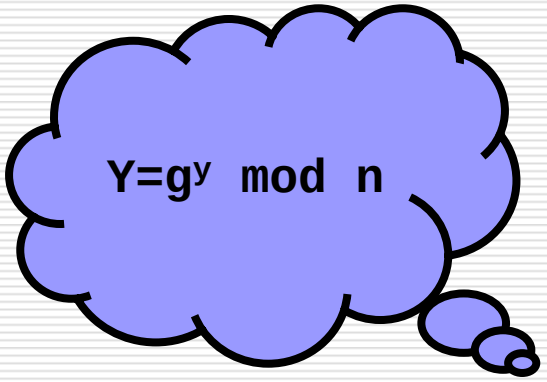
n=13
g=6
y=7

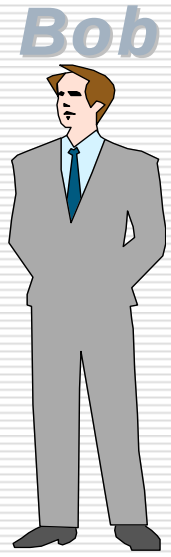
What the hell are they doing now?

Mallory

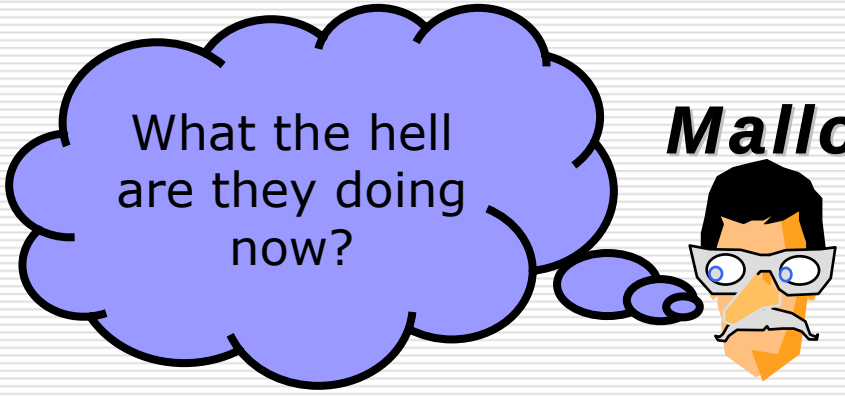
n=13
g=6





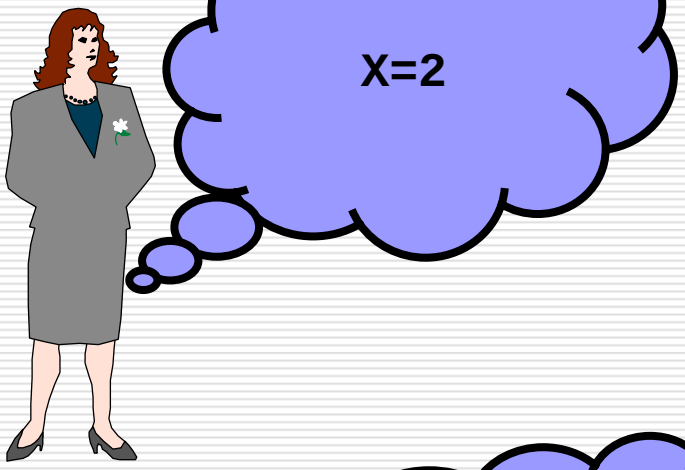


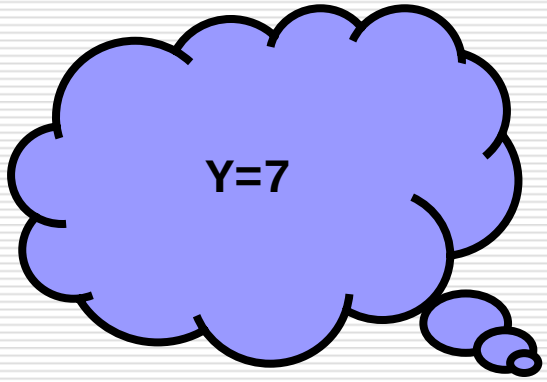
n=13
g=6
x=5

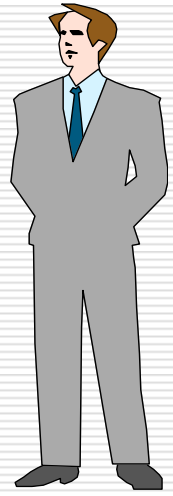


n=13
g=6

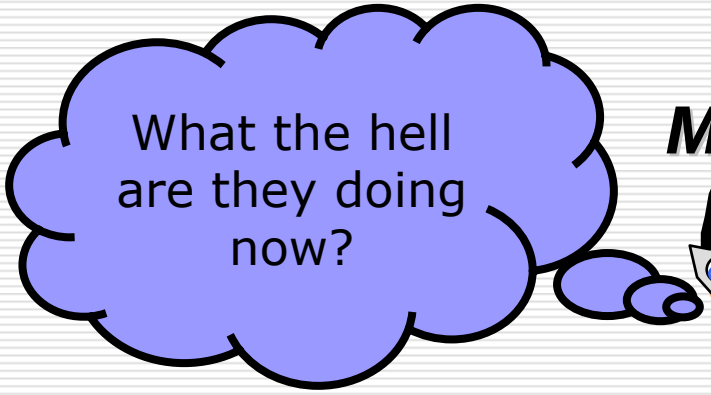
n=13
g=6
y=7







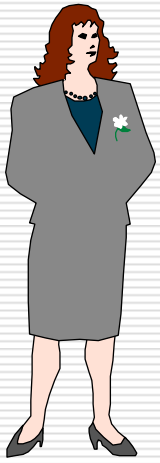
n=13
g=6
x=5
X=2



n=13
g=6

n=13
g=6
y=7
Y=7

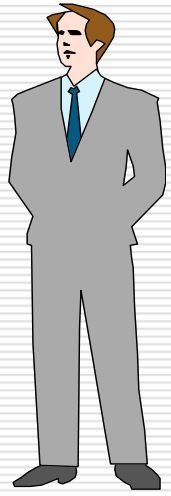
Alice



Bob,
my public
number is **X=2**.

Alice,
my public
number is **Y=7**.

Bob



n=13
g=6
x=5
X=2
Y=7

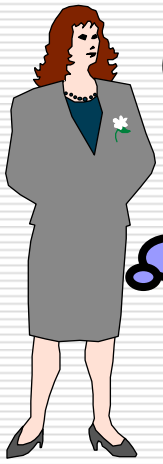
Great,
two aditionally
values!

Mallory

n=13
g=6
X=2
Y=7

n=13
g=6
y=7
Y=7
X=2

Alice

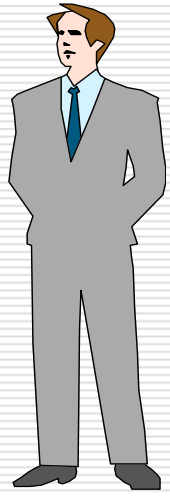


Now I can calculate our shared secret.

n=13
g=6
x=5
X=2
Y=7

Now I can calculate our shared secret.

Bob

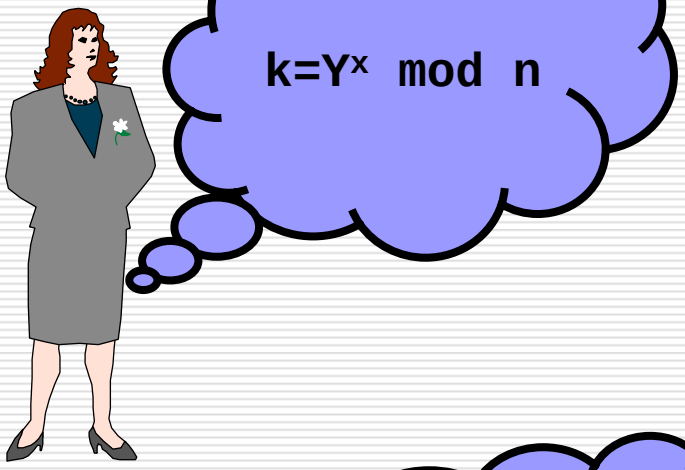


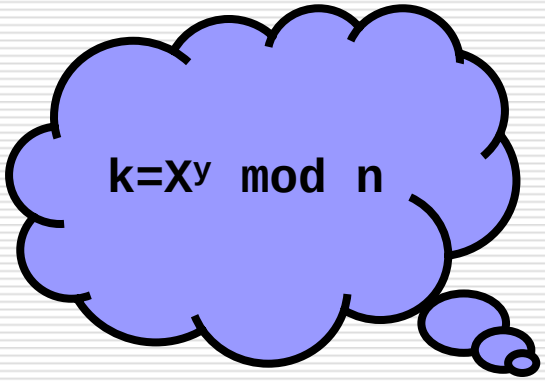
n=13
g=6
y=7
Y=7
X=2

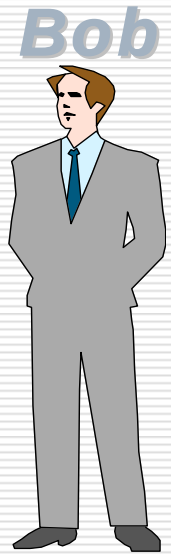
What the hell are they doing now?

Mallory

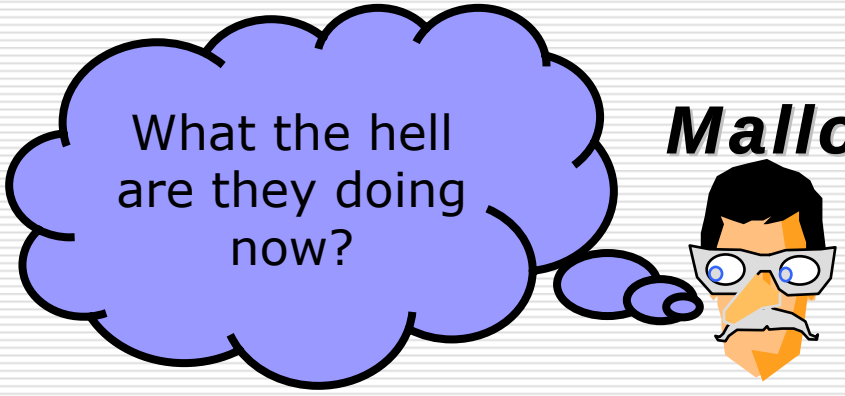
n=13
g=6
X=2
Y=7





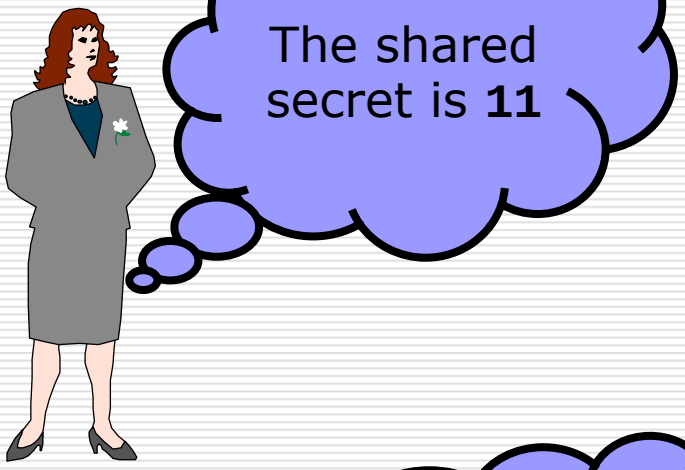


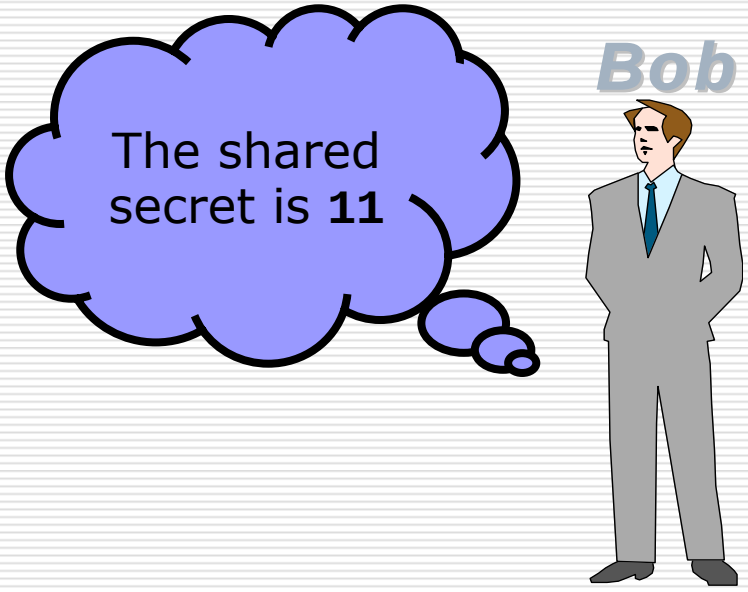
n=13
g=6
x=5
X=2
Y=7



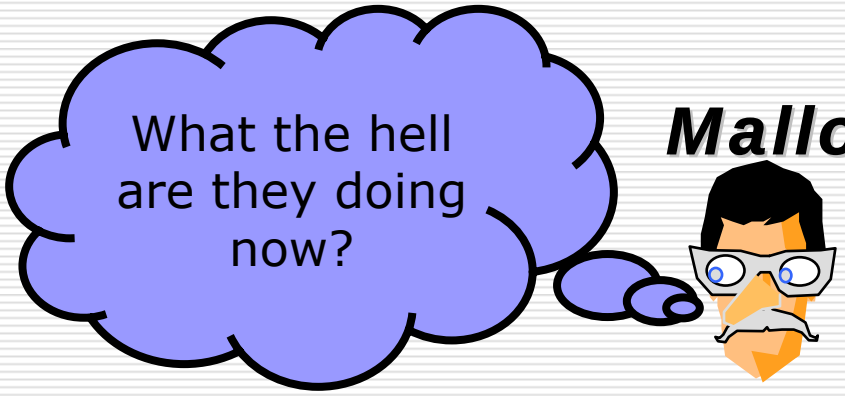
n=13
g=6
X=2
Y=7

n=13
g=6
y=7
Y=7
X=2





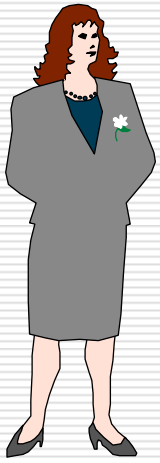
n=13
g=6
x=5
X=2
Y=7
k=11



n=13
g=6
X=2
Y=7

n=13
g=6
y=7
Y=7
X=2
k=11

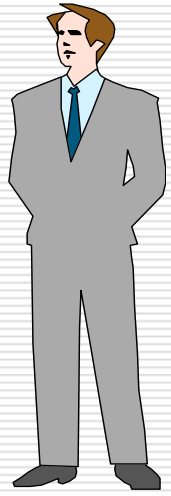
Alice



Now no one will observe our conversation!

Now no one will observe our conversation!

Bob



k=11

k=11

STOP!!!
I can't compute **k** yet!!!

Mallory

n=13
g=6
X=2
Y=7