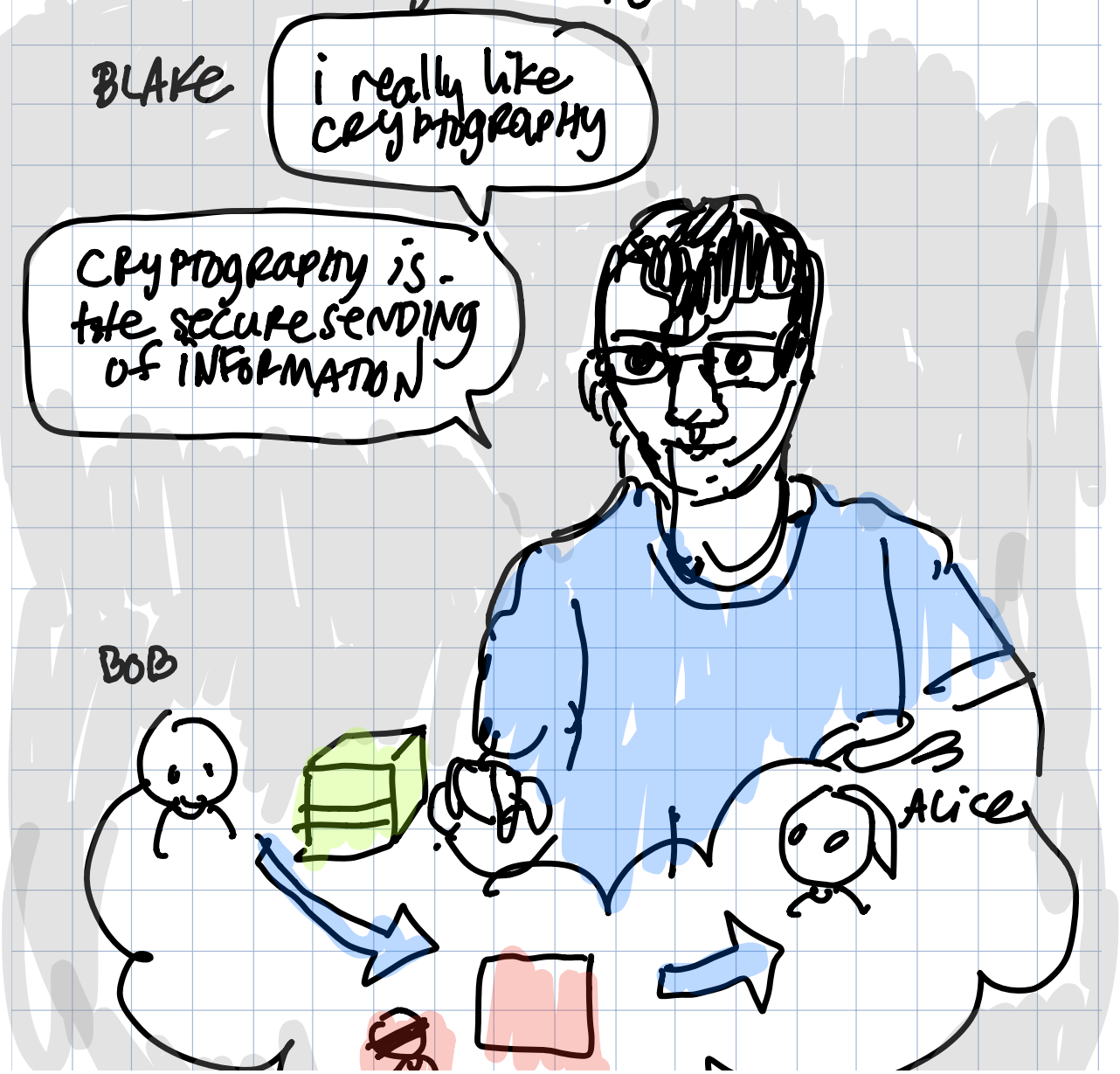
PYTHON

Shannons Principal → Strive to get open source the SECURITY of your library should depend on not having the key - it should never be about not knowing what the algorithm is.

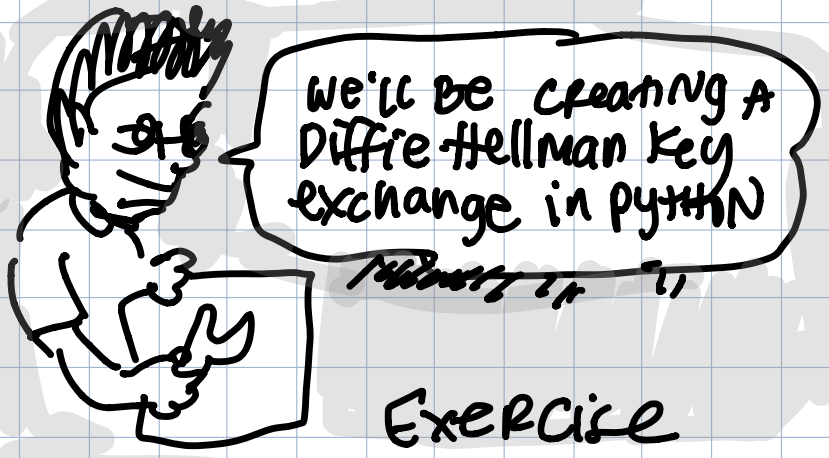


thief

ways to think about cryptography

Asymmetric
AES

Symmetric



Exercise

industry folks drop by to talk about real world uses of python

in transit?

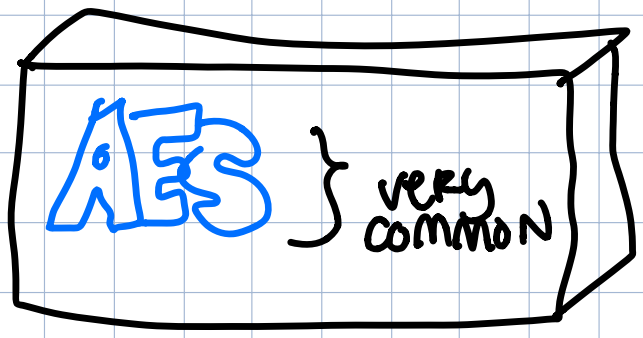
at rest

asymmetric

symmetric

AES

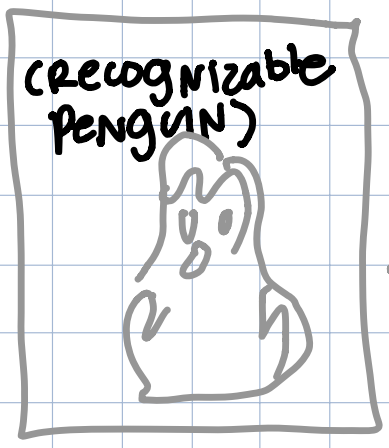
default output
↝ 16 bytes (128 bits)



this is a very common

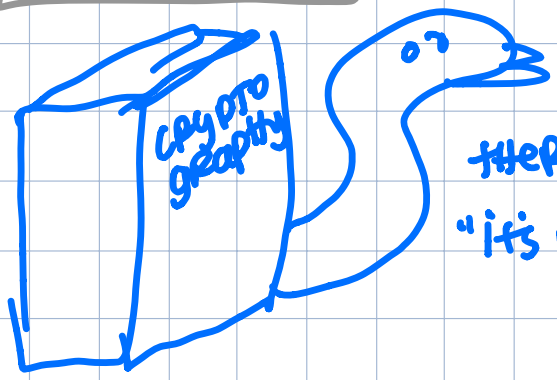
block cypher modes

BUILDING BLOCK



SUBTLETY - SOMETIMES YOU ENCRYPT STUFF BUT YOU CAN STILL RECOGNIZE IT

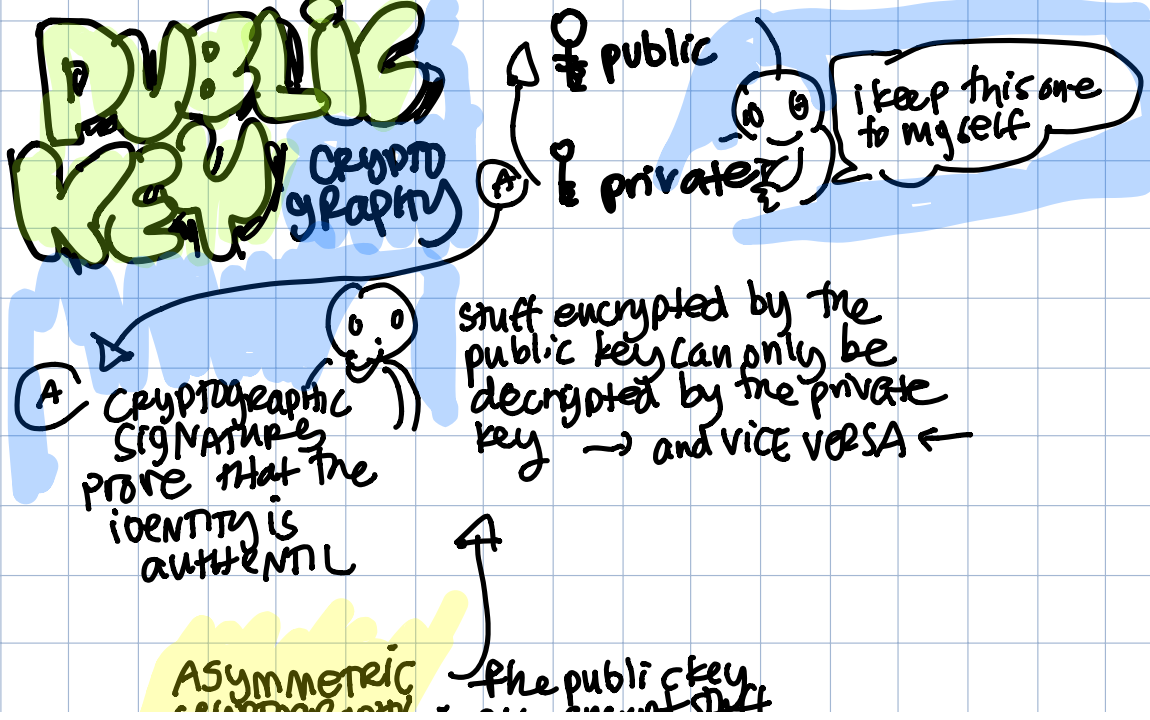
ex. SNAPCHAT



THERE'S A PYTHON LIBRARY "IT'S DANGEROUS"

NEW TERM

PUBLIC KEY CRYPTOGRAPHY



cryptographic example

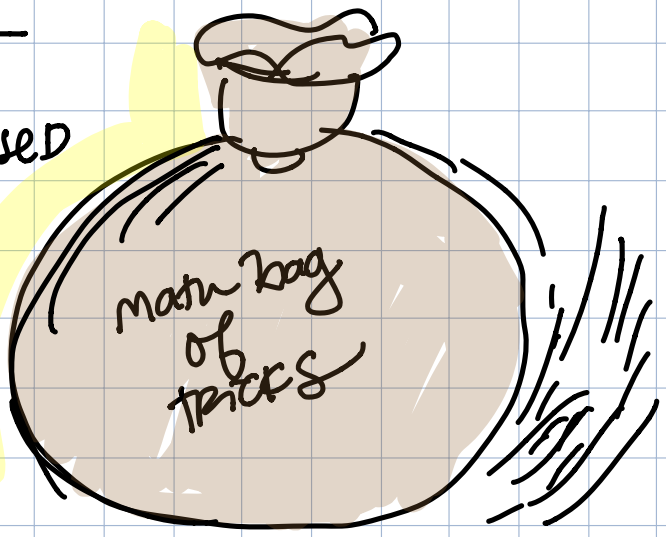
but not unlock it

ex. whenever you establish a TLS connection to a website

MATH CONCEPTS—

the modulo % is used commonly.

there are LOTS of bags of TRICKS



ex. "TRAPDOORS" involve prime numbers and you can discover secrets

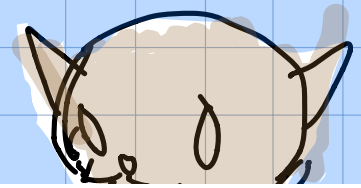
$(5^{***3}) \% 17 =$ result is 6

you might have to brute force this stuff.

diffie hellman uses this technique to discover a secret

$5^{13} \% 17$

$a = g^p \bmod p$ ← this is always a prime



random discussion

it's always

good to review basic math

increasing the randomness requires some forethought

```
import random
random_num = random.randint(0, 100)
```

basic python

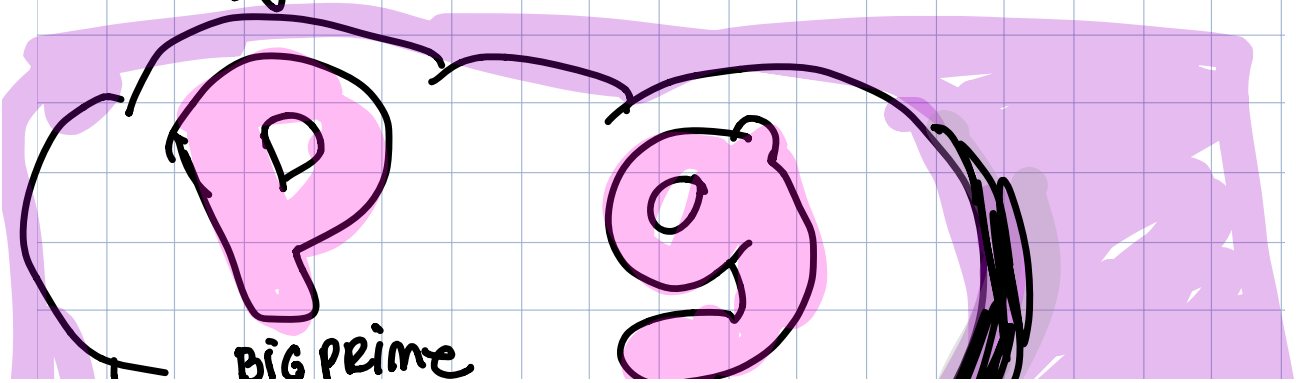
Python is great for handling integers you don't have to code.

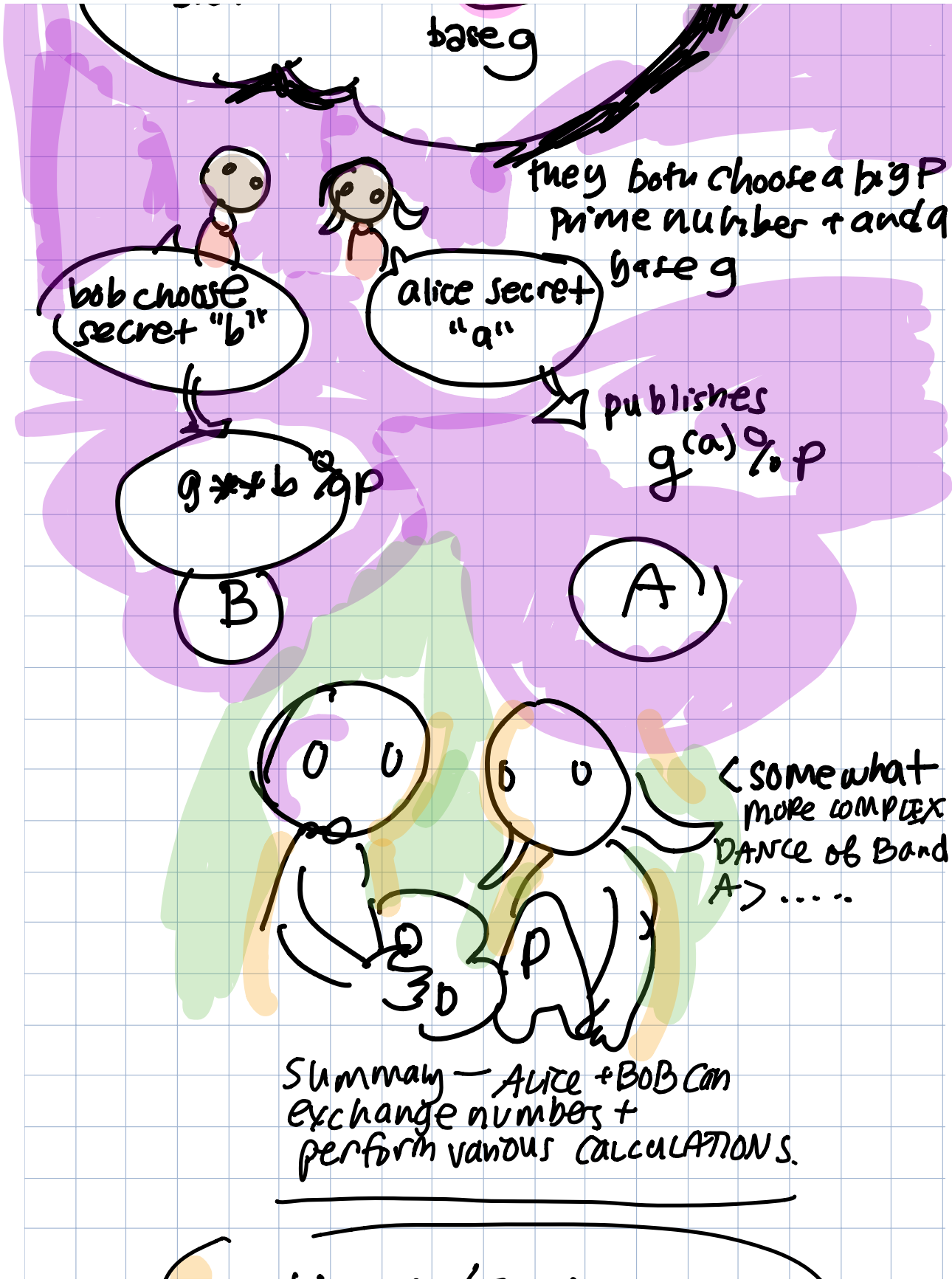
code escape

```
def randint(n, bytes):
    return int.from_bytes(os.urandom(nbytes),
        byteorder='little'
```

//code - probably check the notebook he has.

DIFFIE HELLMAN




base g
they both choose a big P prime number + and g base g
bob choose secret "b"
alice secret "a"
publishes g^(a) % p
g**b %p
B
A
<somewhat more complex DANCE of Band A> ....
P
P
Summary — Alice + BOB can exchange numbers + perform various CALCULATIONS.

pastebin.com/7QARWsFØ

<DISCUSSION of CRYPTOGRAPHY>

symmetric

CRYPTOGRAPHIC BUILDING BLOCK

hasher = sha256()

TODO checkout hashes—
given the OUTPUT CAN'T figure out the INPUT

"SALT" the PASSWORDS if