CS 338

Wed, 27 Sep 2023

$$a^b \bmod n$$

if $b == 2x$

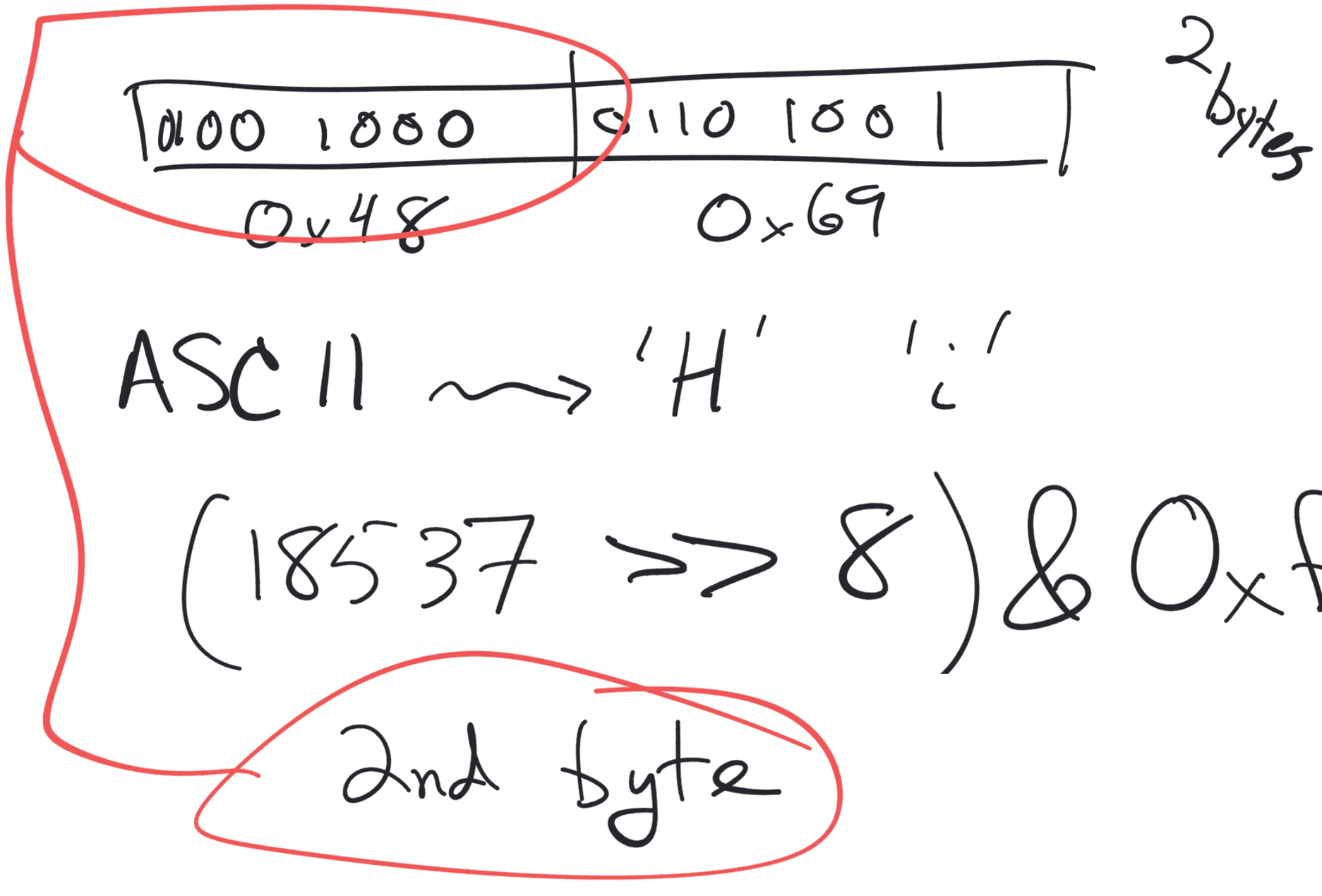
$$a^b \bmod n = a^{2x} \bmod n$$
$$= (a^x \bmod n)^2 \bmod n$$

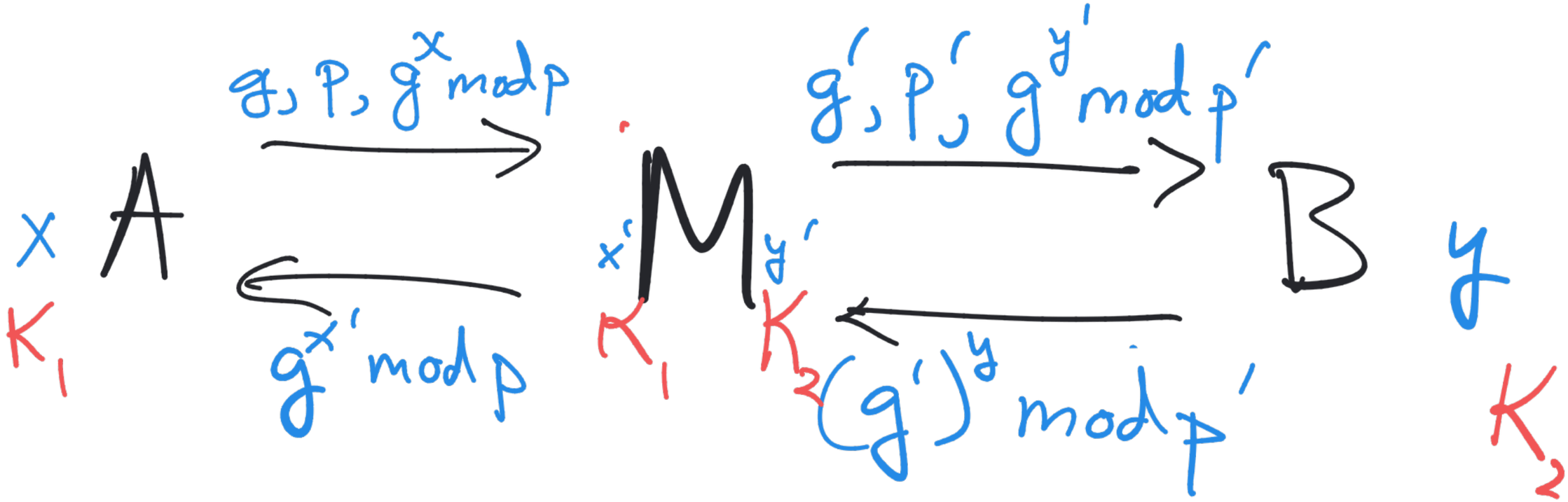
---

if $b == 2y + 1$

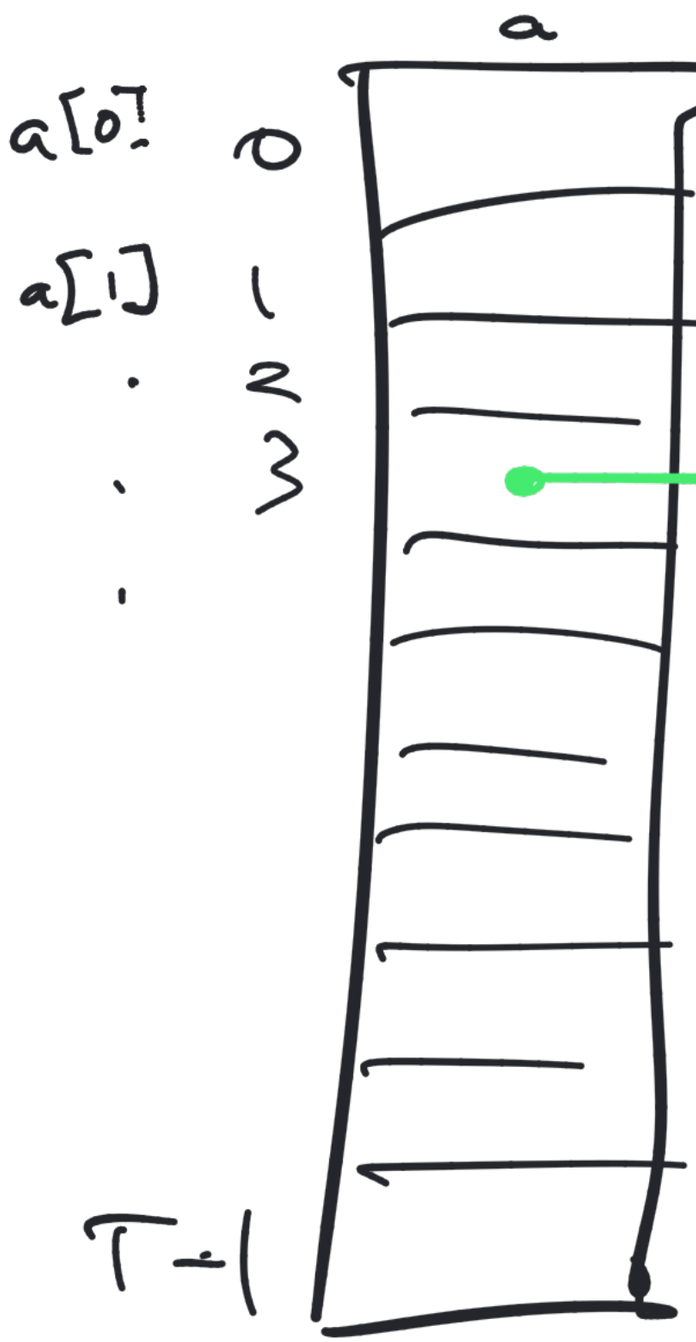
$$a^b \bmod n = a^{2y+1} \bmod n$$
$$= ((a^y \bmod n)^2 \cdot a) \bmod n$$

18537 = 0x4869




g, p, g^x mod p
g', p', g^y' mod p'
x
A
M
B
y
K1
K1'
K2'
K2
g^x' mod p
(g')^y mod p'

Hash table (CS 201)



To insert "marmot"

① $h = \text{hash}(\text{"marmot"}) \bmod 3$

② Look at a[h].
Is "marmot" already there?

③ If not, insert it.

This is not the kind of hash function we'll be talking about

Cryptographic hash function

Standard hashes

obsolete ~~MD5~~

SHA-1

SHA-2

SHA3

SHA-256

SHA-224 ...

bcrypt

Asymmetric encryption

Public key : P

Secret/private key : S

Encryption algorithm : E(block, key)

Ciphertext = E(plaintext, P)

only the holder(s) of S
can get the plaintext back

Digital Signature

P_{Bob}, S_{Bob}, E, $h = SHA256$

Message M not to be encrypted

Bob sends: $M \,||\, E(h(M), S_{Bob})$

Sig

$||$ → Concatenation

only Bob could compute this

Verifying a sig.

Alice has

M, sig, P_{Bob}, E

Question: is sig $\stackrel{?}{=} E(h(M), S_{Bob})$

Alice can't compute this

$E(sig, P_{Bob})$

if sig ==

then

$E(sig, P_{Bob}) = E(E(h(M)), S_{Bob}), P_{Bob})$

Alice can compute

$= h(M)$