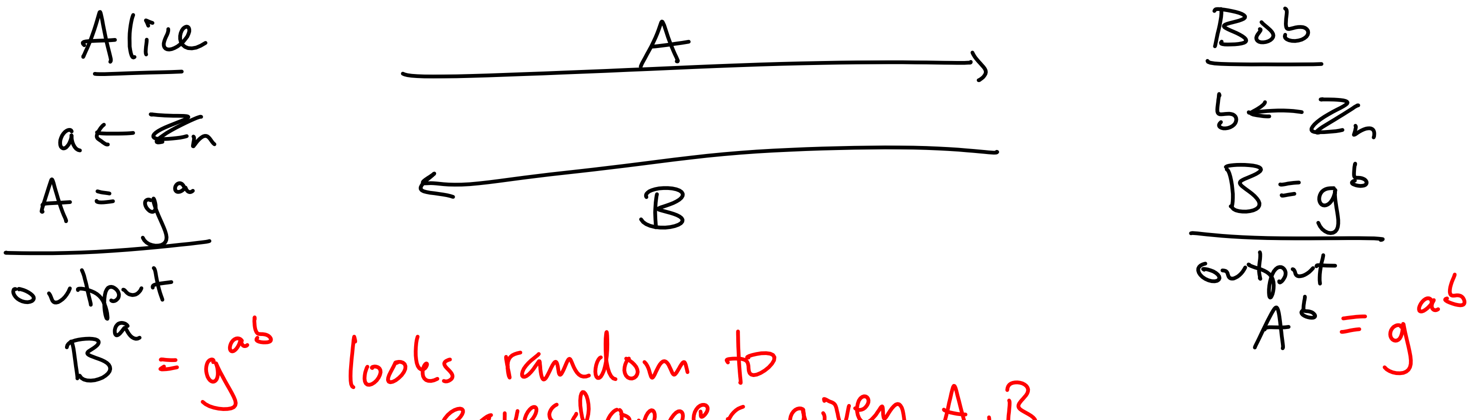
El Gamal & Hybrid Enc

DHKA:

params: g : generator of cyclic group
(e.g, $\langle g \rangle = \mathbb{Z}_p^*$ for prime p)

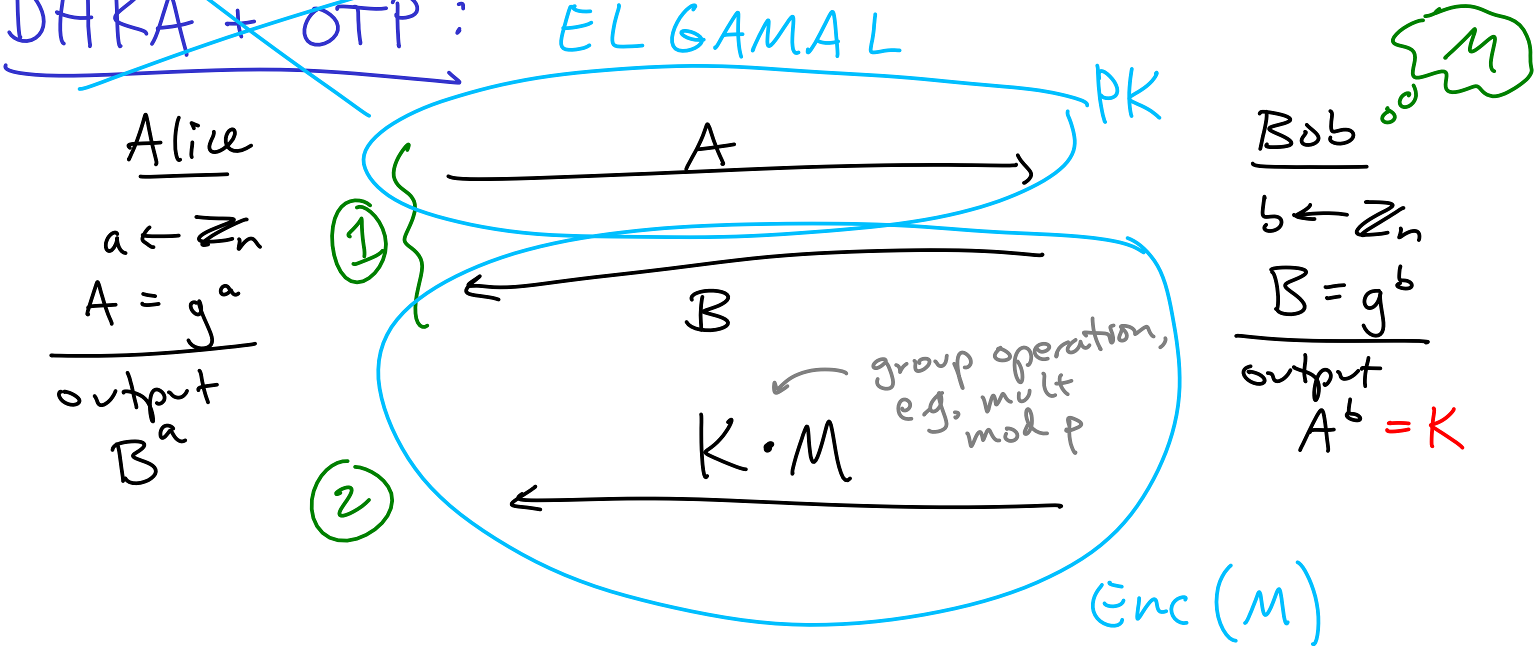


looks random to eavesdropper given A, B

What if: Bob wants to send secret msg to Alice?

Idea: ① Run DHKA $\rightsquigarrow$ K that only they know
use K as OTP to send msg
↪ OTP in cyclic group using multiplication mod p, not ⊕

~~DHKA + OTP~~ : EL GAMAL


M
Alice
$a \leftarrow \mathbb{Z}_n$
$A = g^a$
output
B^a
PK
A
①
B
②
$K \cdot M$
group operation, e.g, mult mod p
Enc (M)
Bob
$b \leftarrow \mathbb{Z}_n$
$B = g^b$
output
$A^b = K$

ElGamal:

KeyGen:

$a \leftarrow \mathbb{Z}_n$ private

$A = g^a$ public

Enc(pk, M):

mult mod p

$$\left.\begin{aligned} b &\leftarrow \mathbb{Z}_n \\ B &= g^b \\ C &= M \cdot A^b \end{aligned}\right\} \text{ciphertext}$$

Dec(sk, (B, C)):

compute $K = B^a$

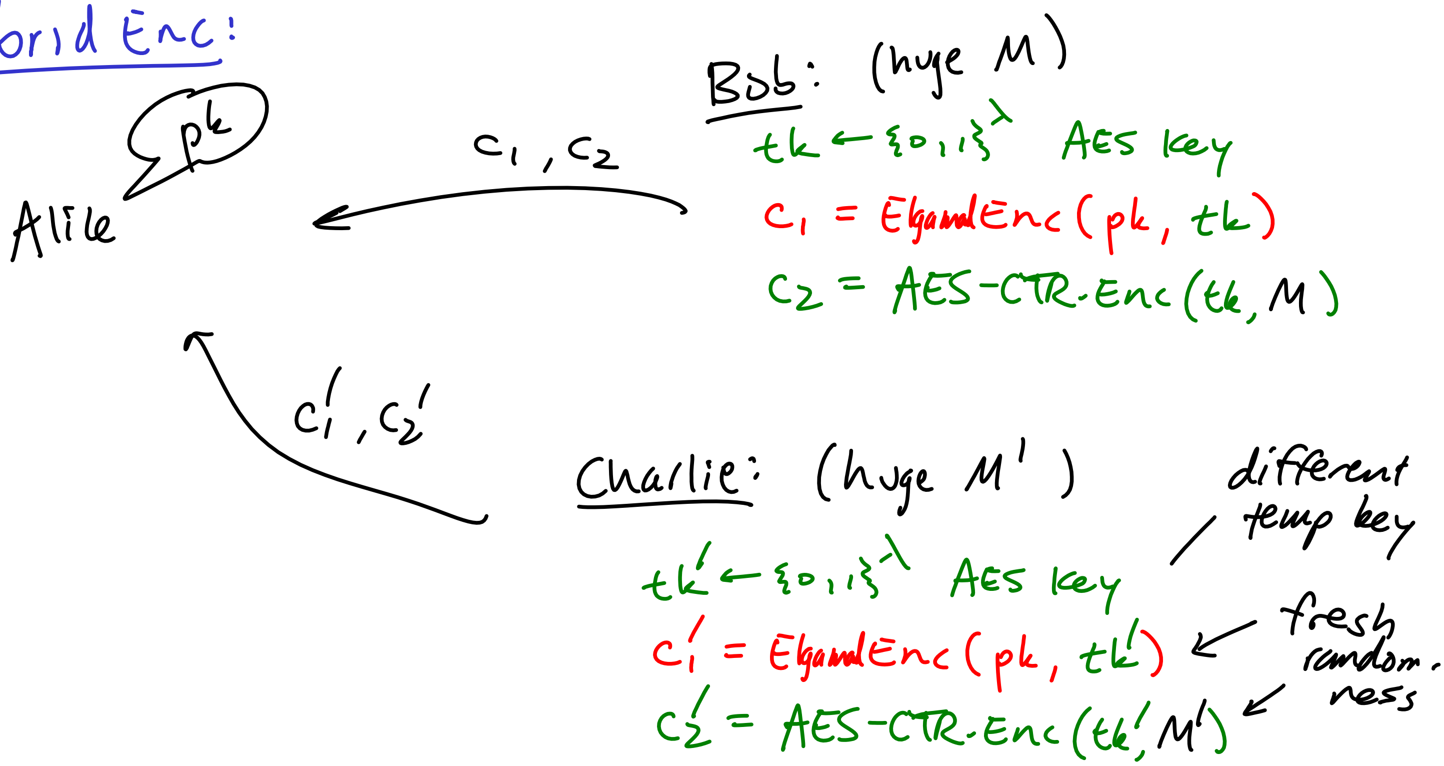
return $C \cdot \underbrace{K^{-1}}$ inverse mod p

1/Mod(K,p)

Cost of Encryption: (CPA)

symmetric key:	AES-CTR	costs 1 cycle per bit
public-key:	ElGamal	costs gazillions

Hybrid Enc:



Bob: (huge M)

$tk \leftarrow \{0,1\}^\lambda$ AES key

$c_1 = \text{ElgamalEnc}(pk, tk)$

$c_2 = \text{AES-CTR.Enc}(tk, M)$

Charlie: (huge M')

different temp key

$tk' \leftarrow \{0,1\}^\lambda$ AES key

$c_1' = \text{ElgamalEnc}(pk, tk')$

$c_2' = \text{AES-CTR.Enc}(tk', M')$

fresh random-ness

Q: Why is this secure? (CPA)

A: main "payload" (M) is encrypted under AES-CTR, which is CPA-secure (c_2 hides M)

Q: CPA security applies only when key is used nowhere else, but here AES-CTR uses tk as key and tk is used elsewhere ☆

A: tk used only as ptxt for CPA-secure ElGamal, so c_1 hides tk — it's like tk is not being used at all

---

① important that k public

⇒ attacker can compute $F^{-1}(k, \cdot)$

② N vs $\phi(N)$: pari has sqrtint

③ end game: do $\gcd(x, N)$

where x is mult of p

x is NOT mult of q

then $\gcd(x, N) = p$

so find x w/ this property

(similar to what we did
w/ sqrts of unity)