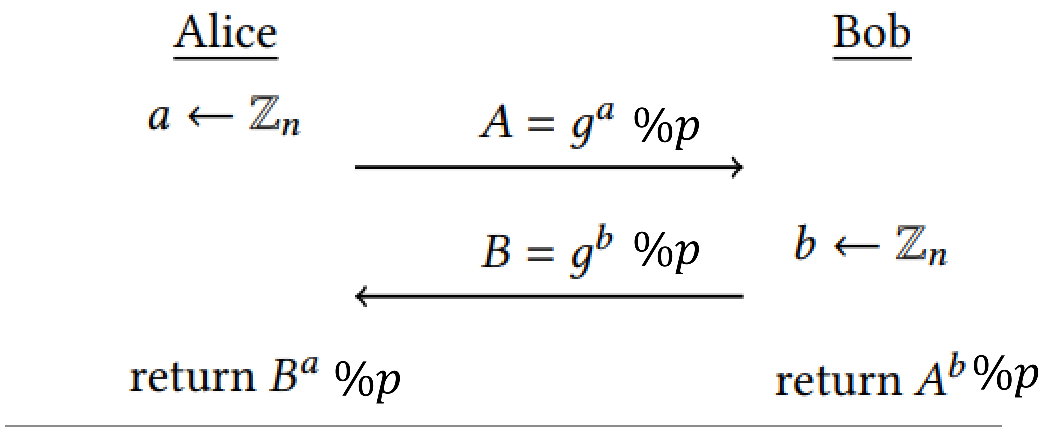
CSE 539: Applied Cryptography
Week 9: Public-Key Encryption

Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap15.pdf

Recap: DHKE



Alice

Bob

$a \leftarrow \mathbb{Z}_n$

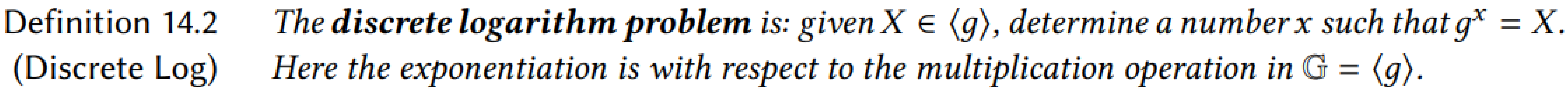
$A = g^a \ \%p$

$B = g^b \ \%p$

$b \leftarrow \mathbb{Z}_n$

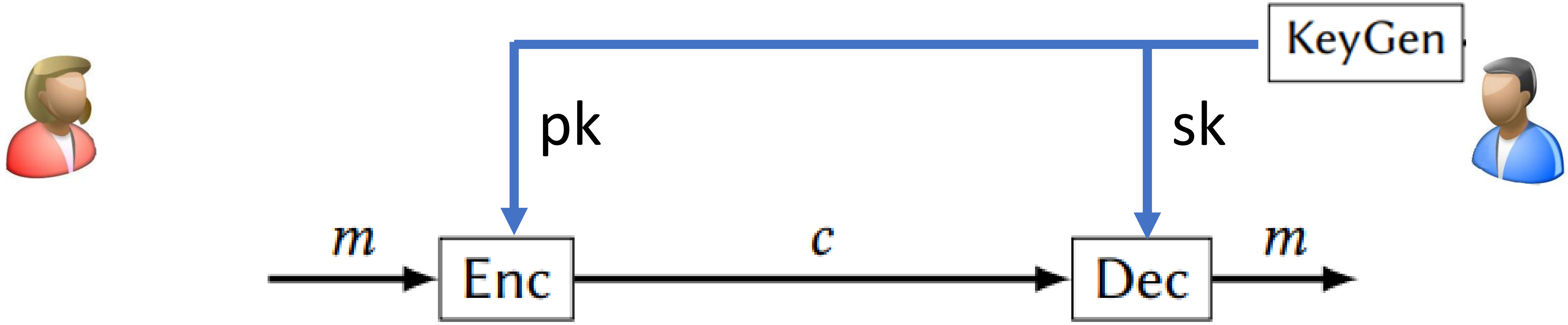
return $B^a \ \%p$

return $A^b \%p$

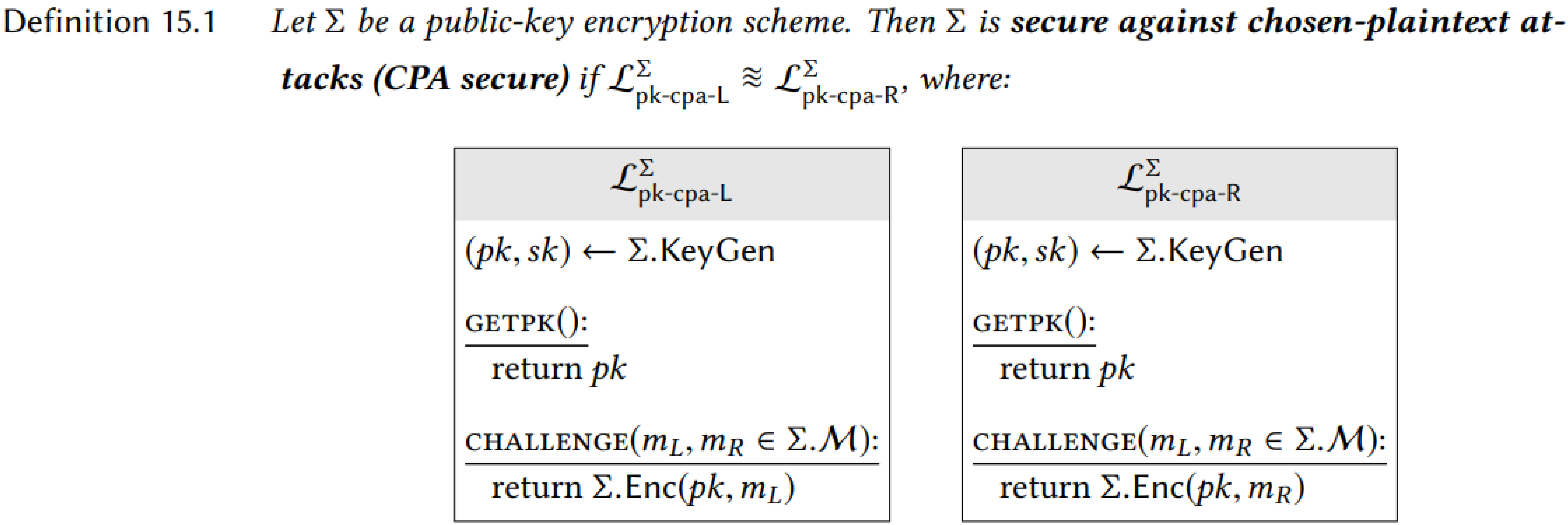


Definition 14.2 (Discrete Log) *The **discrete logarithm problem** is: given $X \in \langle g \rangle$, determine a number x such that $g^x = X$. Here the exponentiation is with respect to the multiplication operation in $\mathbb{G} = \langle g \rangle$.*

Public Key



Public Key

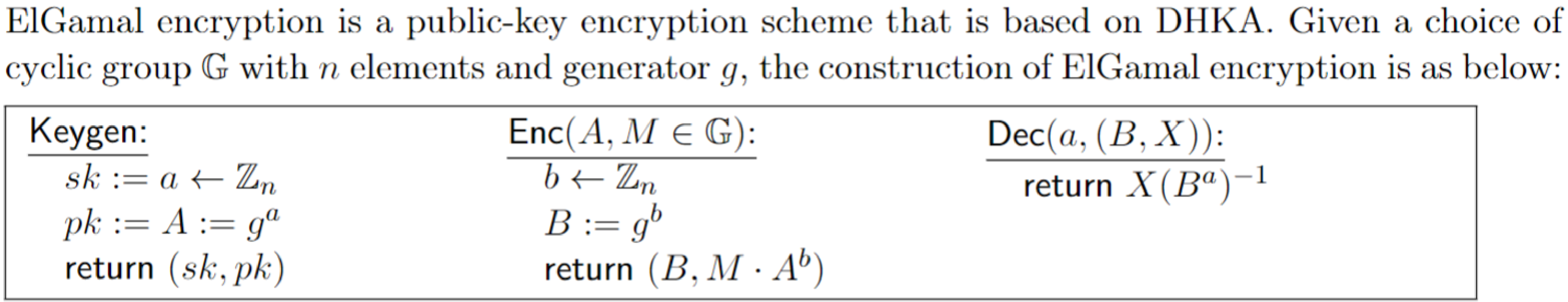


Definition 15.1 *Let Σ be a public-key encryption scheme. Then Σ is **secure against chosen-plaintext attacks (CPA secure)** if $\mathcal{L}^{\Sigma}_{\text{pk-cpa-L}} \approx \mathcal{L}^{\Sigma}_{\text{pk-cpa-R}}$, where:*

```
$\mathcal{L}^{\Sigma}_{\text{pk-cpa-L}}$
$(pk, sk) \leftarrow \Sigma.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
    return $pk$

$\underline{\textsc{challenge}(m_L, m_R \in \Sigma.\mathcal{M}):}$
    return $\Sigma.\text{Enc}(pk, m_L)$
```

```
$\mathcal{L}^{\Sigma}_{\text{pk-cpa-R}}$
$(pk, sk) \leftarrow \Sigma.\text{KeyGen}$

$\underline{\textsc{getpk}():}$
    return $pk$

$\underline{\textsc{challenge}(m_L, m_R \in \Sigma.\mathcal{M}):}$
    return $\Sigma.\text{Enc}(pk, m_R)$
```

Public Key: ElGamal Encryption

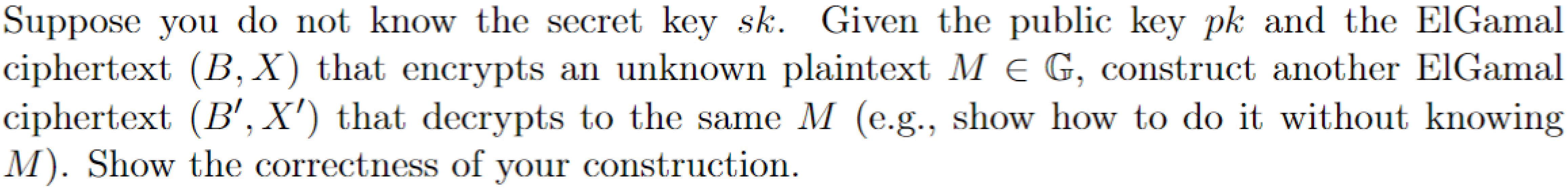


ElGamal encryption is a public-key encryption scheme that is based on DHKA. Given a choice of cyclic group $\mathbb{G}$ with n elements and generator g, the construction of ElGamal encryption is as below:

```
Keygen:
    $sk := a \leftarrow \mathbb{Z}_n$
    $pk := A := g^a$
    return $(sk, pk)$

Enc$(A, M \in \mathbb{G})$:
    $b \leftarrow \mathbb{Z}_n$
    $B := g^b$
    return $(B, M \cdot A^b)$

Dec$(a, (B, X))$:
    return $X(B^a)^{-1}$
```

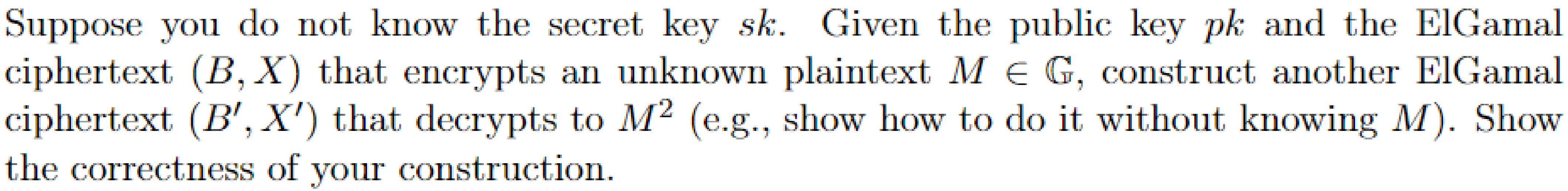
ElGamal Encryption vs DHKE

ElGamal Encryption



Suppose you do not know the secret key sk. Given the public key pk and the ElGamal ciphertext (B, X) that encrypts an unknown plaintext $M \in \mathbb{G}$, construct another ElGamal ciphertext (B', X') that decrypts to the same M (e.g., show how to do it without knowing M). Show the correctness of your construction.

ElGamal Encryption



Suppose you do not know the secret key sk. Given the public key pk and the ElGamal ciphertext (B, X) that encrypts an unknown plaintext $M \in \mathbb{G}$, construct another ElGamal ciphertext (B', X') that decrypts to M^2 (e.g., show how to do it without knowing M). Show the correctness of your construction.