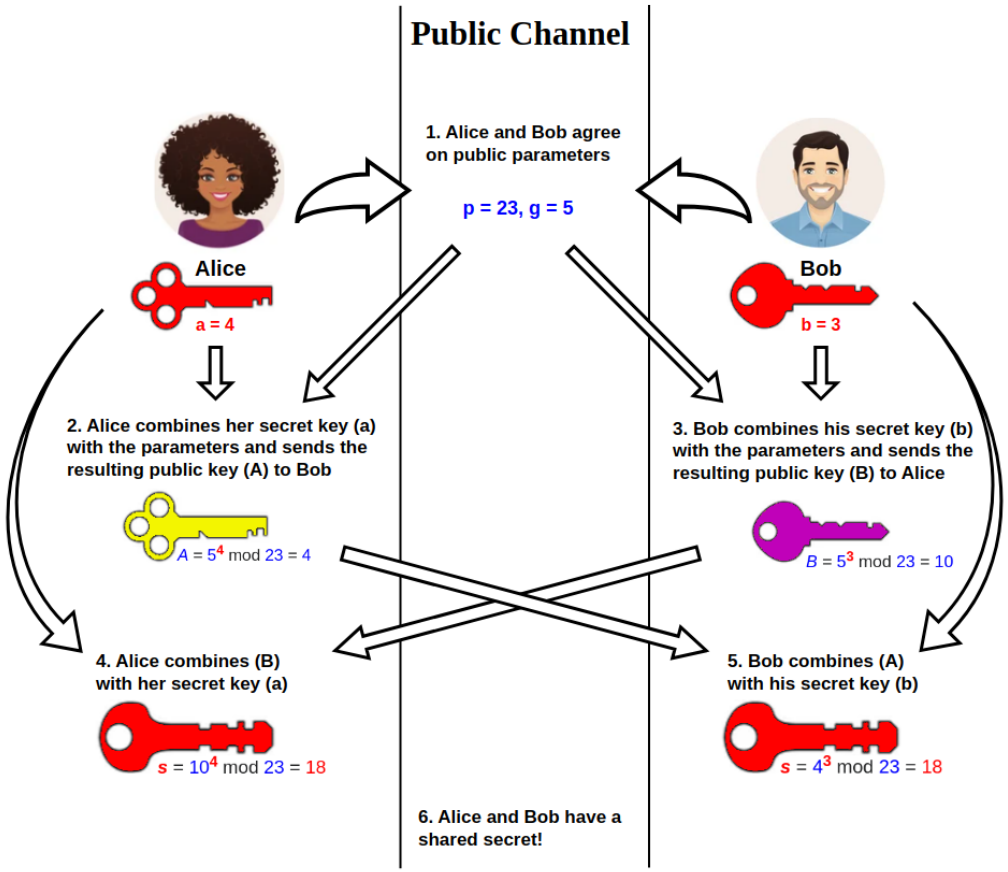
CS553: Crypto In Action Series

Image Source: Dall-E



CS 553

CRYPTOGRAPHY

CIA: Crypto In Action

Secure Key Encapsulation

Instructor
Dr. Dhiman Saha

Image Source: https://upload.wikimedia.org/wikipedia/commons/c/c8/DiffieHellman.png

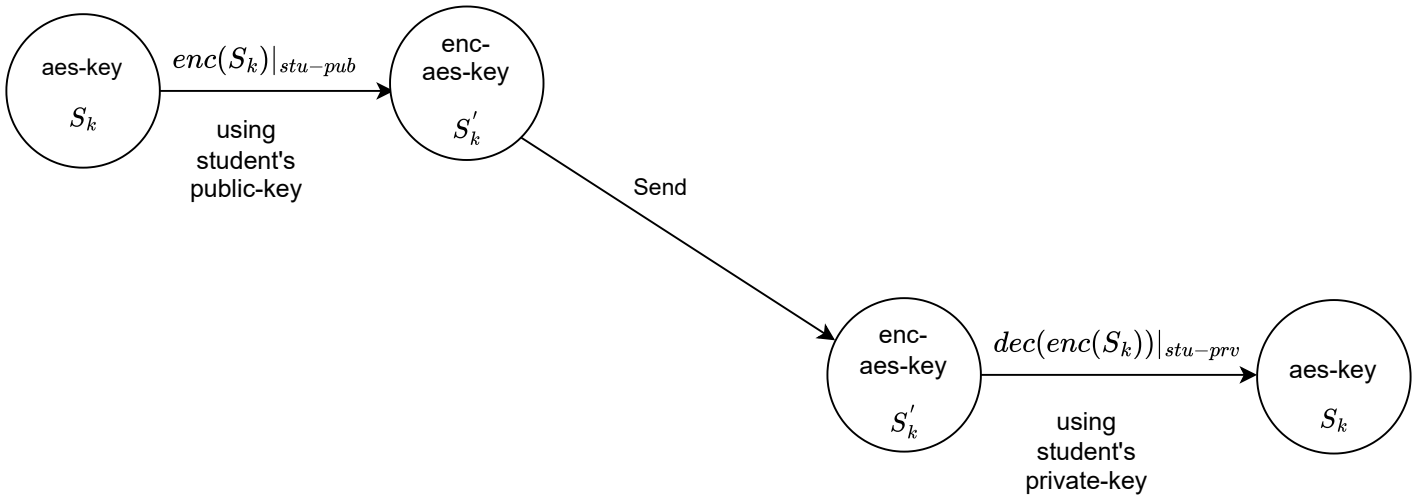
Key Encapsulation

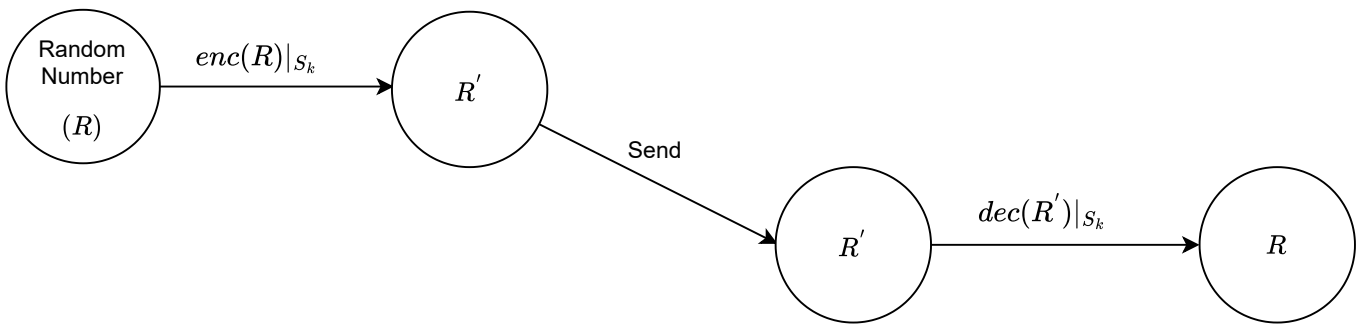
Key encapsulation is a cryptographic mechanism where

a symmetric key is securely shared using asymmetric encryption.

- Sender encrypts the AES key using the recipient's public key.
- Recipient decrypts it with their private key to obtain the AES key.

What Will Do


aes-key
S_k
$enc(S_k)|_{stu-pub}$
using
student's
public-key
enc-
aes-key
S_k'
Send
enc-
aes-key
S_k'
$dec(enc(S_k))|_{stu-prv}$
using
student's
private-key
aes-key
S_k


Random
Number
(R)
$enc(R)|_{S_k}$
R'
Send
R'
$dec(R')|_{S_k}$
R

We have a AES-KEY in file :- aes_key.bin

- Encrypt AES Key with Student's Public Key

```
openssl pkeyutl -encrypt -inkey student_pub_key.pem
-pubin -in aes_key.bin -out enc_aes_key.bin
```

- Send the Encrypted AES Key to the Students.

- Decrypt AES Key Using Private Key

```
openssl pkeyutl -decrypt -inkey student_prv.pem
-in enc_aes_key.bin -out aes_key.bin
```

- Each student will now have the AES key (K1).
- **Next Step**: Use this AES key to decrypt the next message from the TA.

- Generate a Random 128-Bit Number

```
openssl rand -hex 16 > random_num.bin
```

- Encrypt the Random Number with the AES Key (K1)

```
openssl enc -aes-128-cbc -K $(cat aes_key.bin)
-iv 00000000000000000000000000000000
-in random_num.bin -out enc_random_num.bin
```

- Send the Encrypted Random Number to the Students

- Decrypt the Encrypted Random Number Using the AES Key (K1)

```
openssl enc -d -aes-128-cbc -K $(cat aes_key.bin)
-iv 00000000000000000000000000000000
-in enc_random_num.bin -out decrypted_num.bin
```

- Send the Decrypted Random Number Back to the TA.
- TA's will Verify the Random Number Received from Students.