Digital Envelope

Project Report: CSL505 Cryptography
Instructor: Dr Dhiman Saha

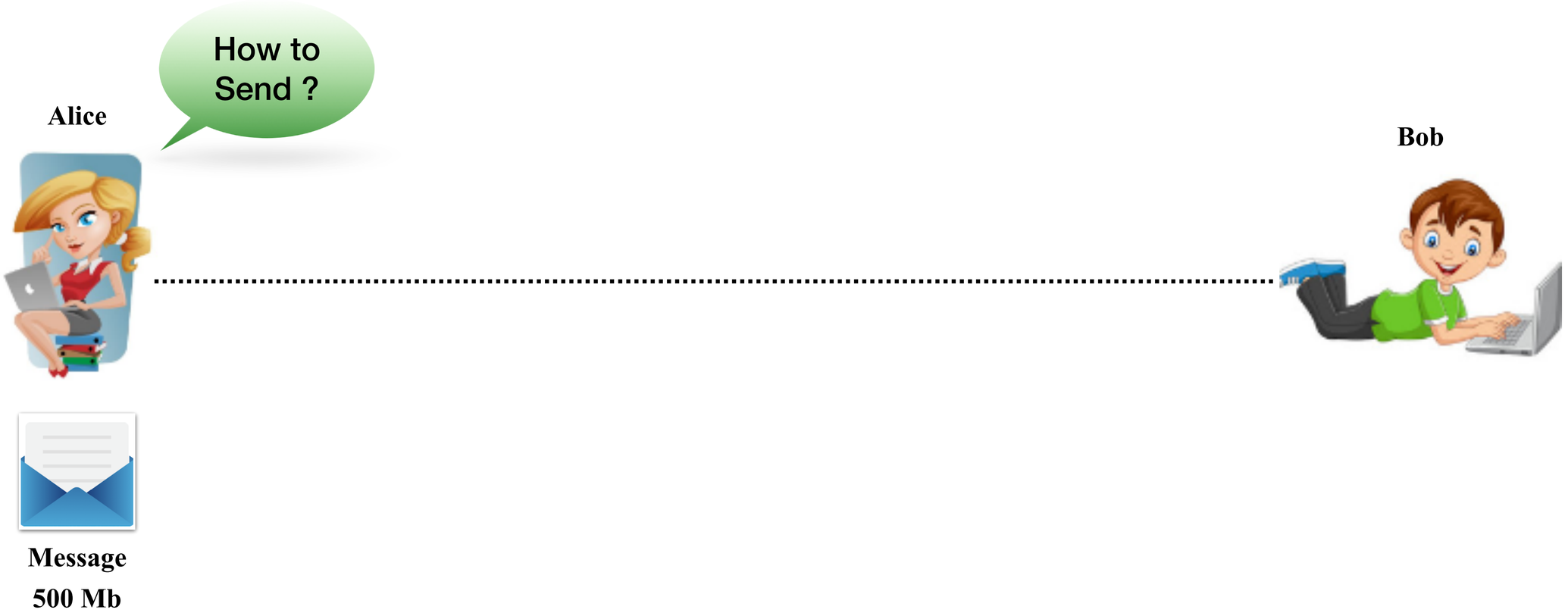
Abu Talha & Vipin Kumar (CSE, IIT Bhilai, CG, India)

10th December 2023

Outlines

- Digital Envelopes
- Why Digital Envelopes
- Applications
- Demonstration of Implementation: An RSA-AES based Digital Envelope (Python)
- Conclusion

The Problem

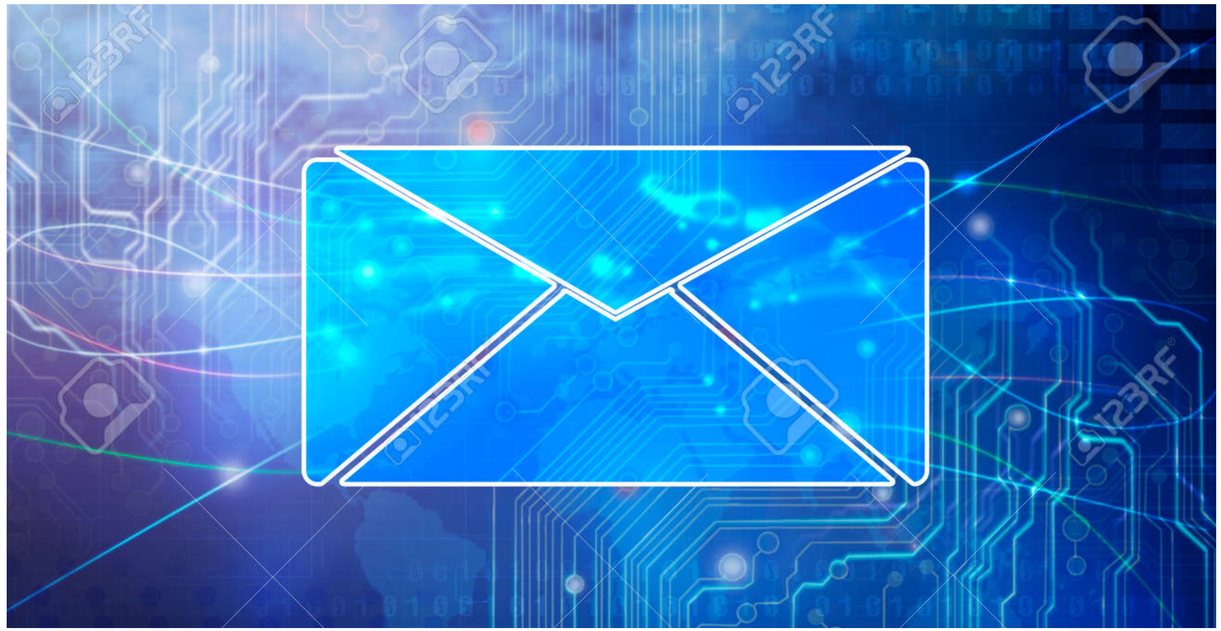


Objective/Motivation

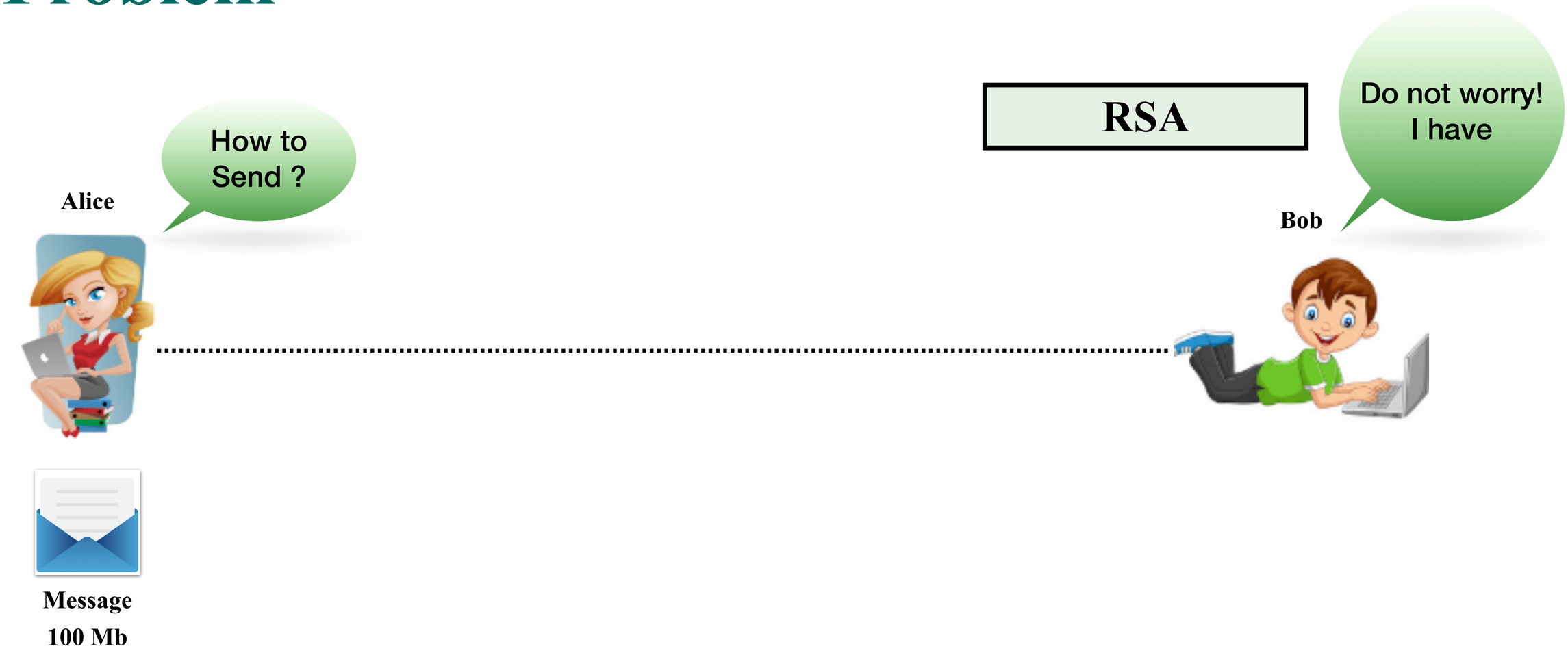
- How to securely transfer a large file over Internet?
- The problem frequently arises in real-world day-to-day scenario.
- Digital Envelope solves it by establishing secure communication.
- Demonstrate the practical implementation of modern cryptographic protocols.

Digital Envelope

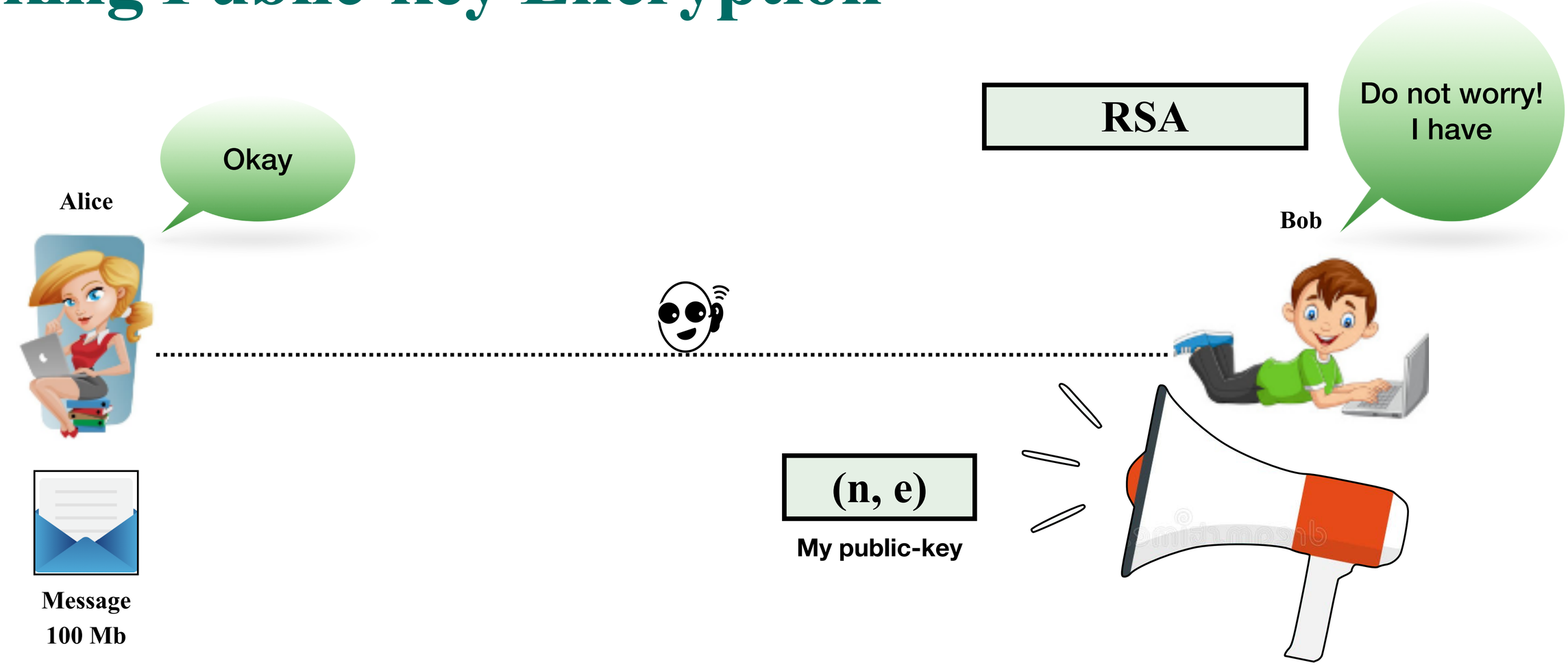
It is a ***secure electronic data container*** that is used to protect the privacy, integrity and authentication of message through the combined used of ***public-key cryptography*** and ***symmetric-key cryptography.***



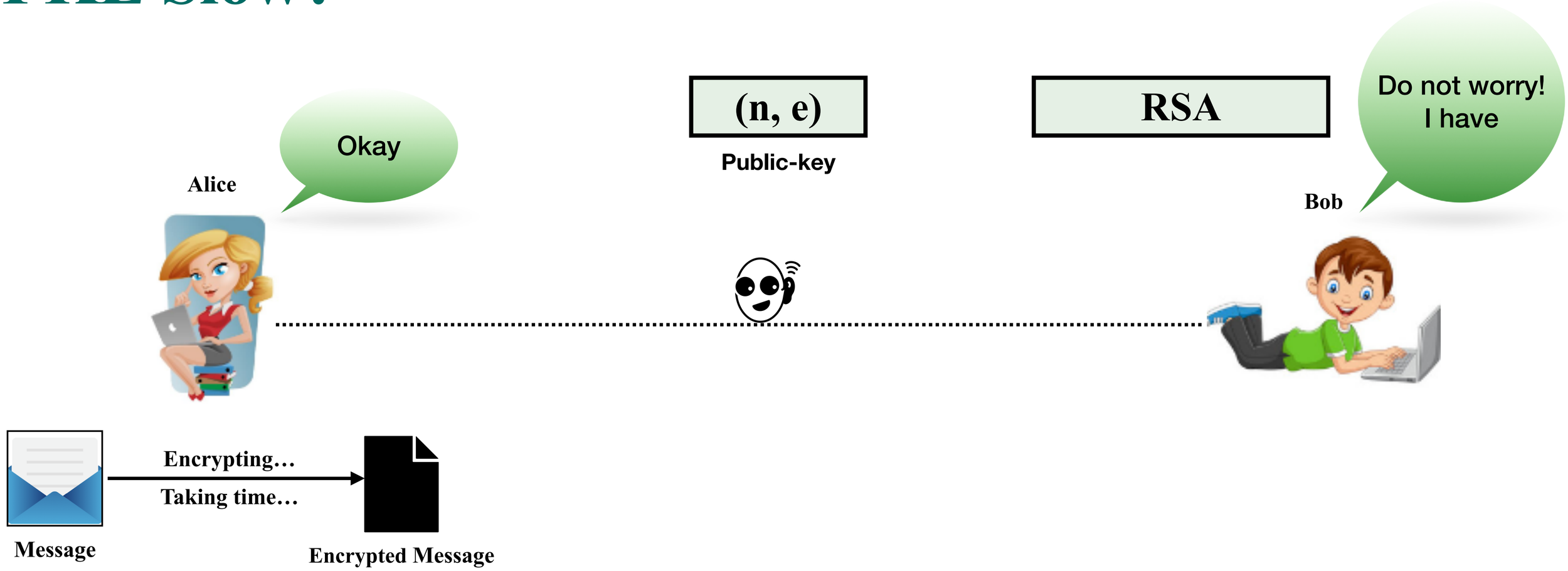
The Problem



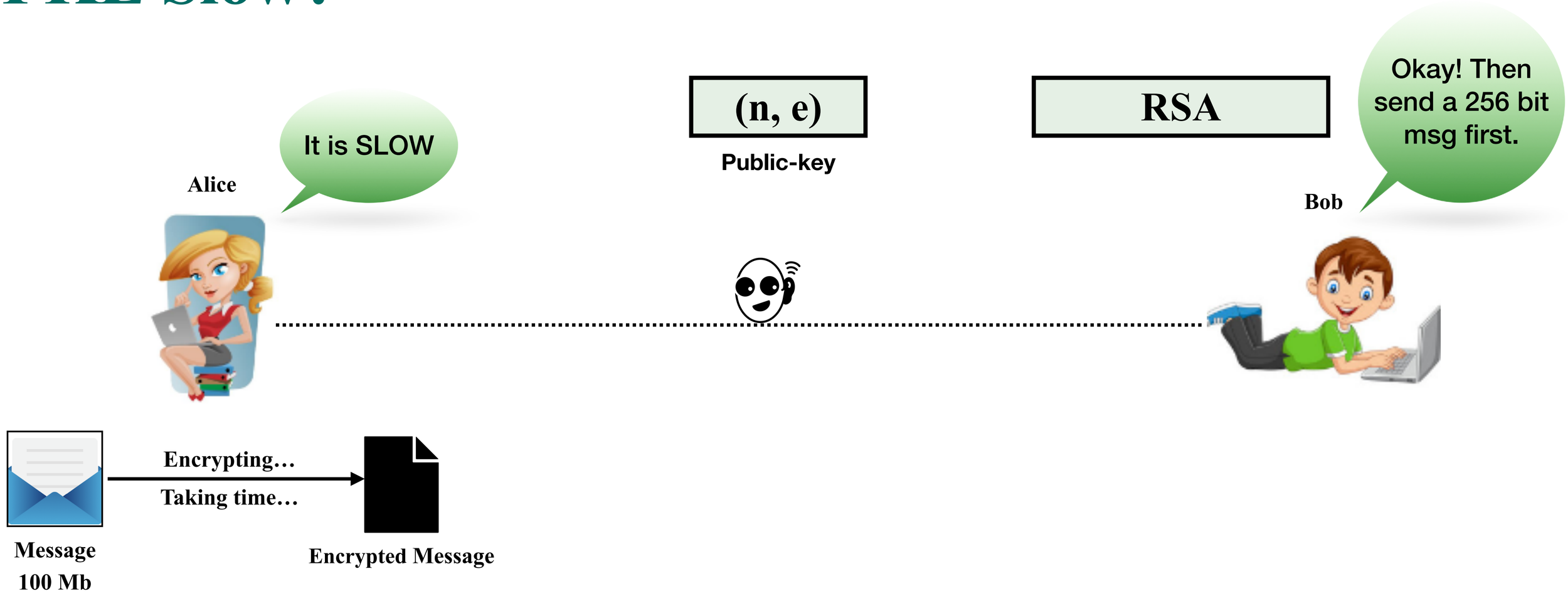
Invoking Public-key Encryption



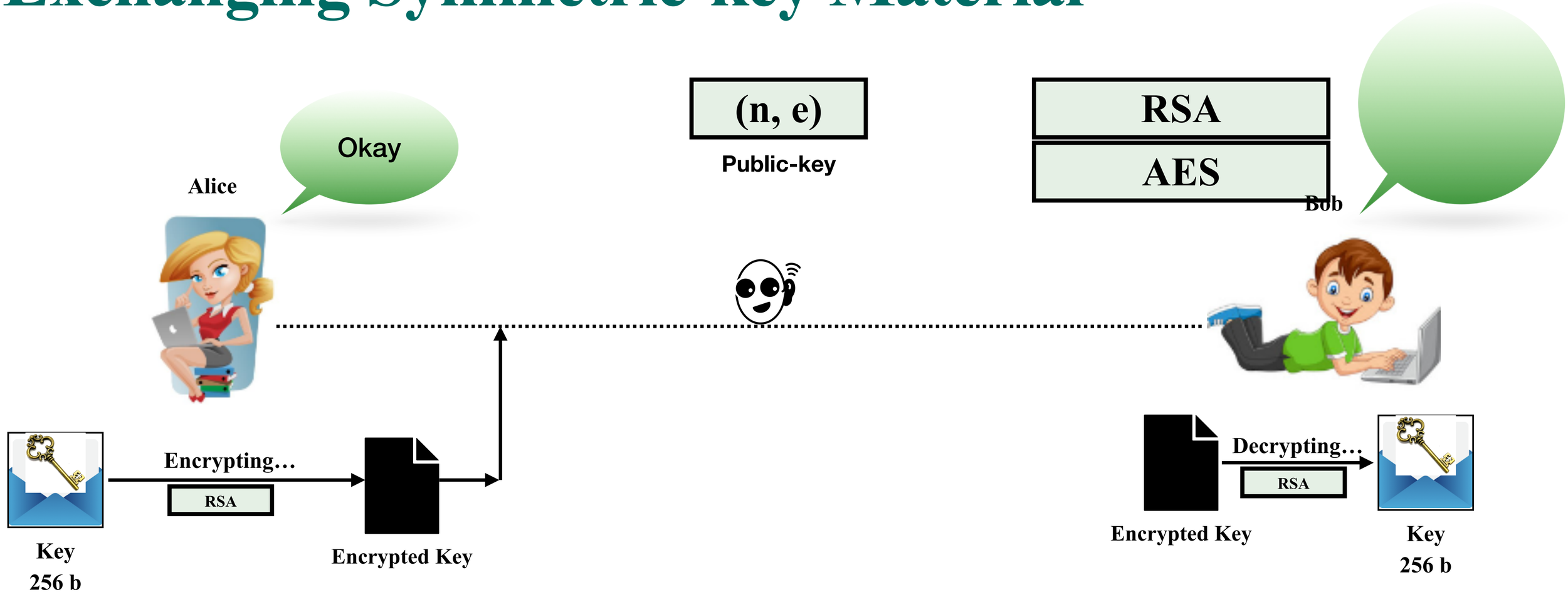
PKE Slow?


Okay
Alice
(n, e)
Public-key
RSA
Do not worry!
I have
Bob
Encrypting…
Taking time…
Message
100 Mb
Encrypted Message

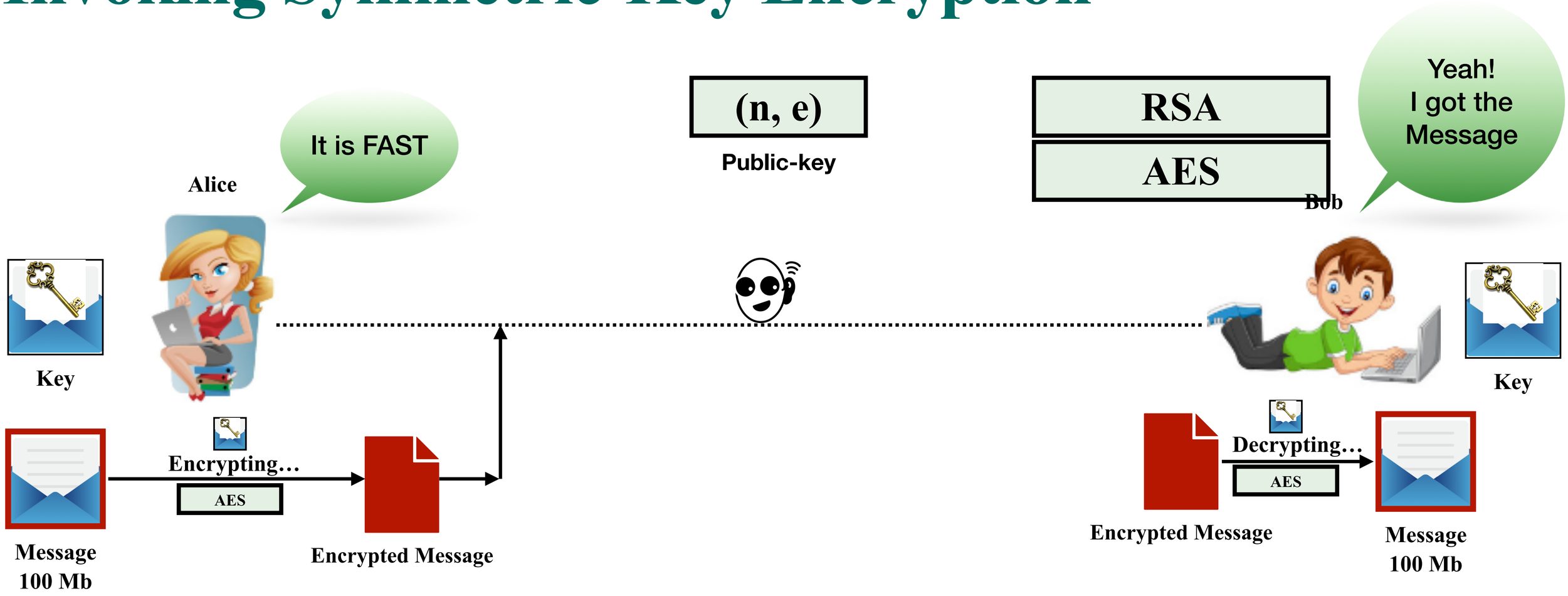
PKE Slow?


It is SLOW
Alice
(n, e)
Public-key
RSA
Okay! Then send a 256 bit msg first.
Bob
Encrypting…
Taking time…
Message
100 Mb
Encrypted Message

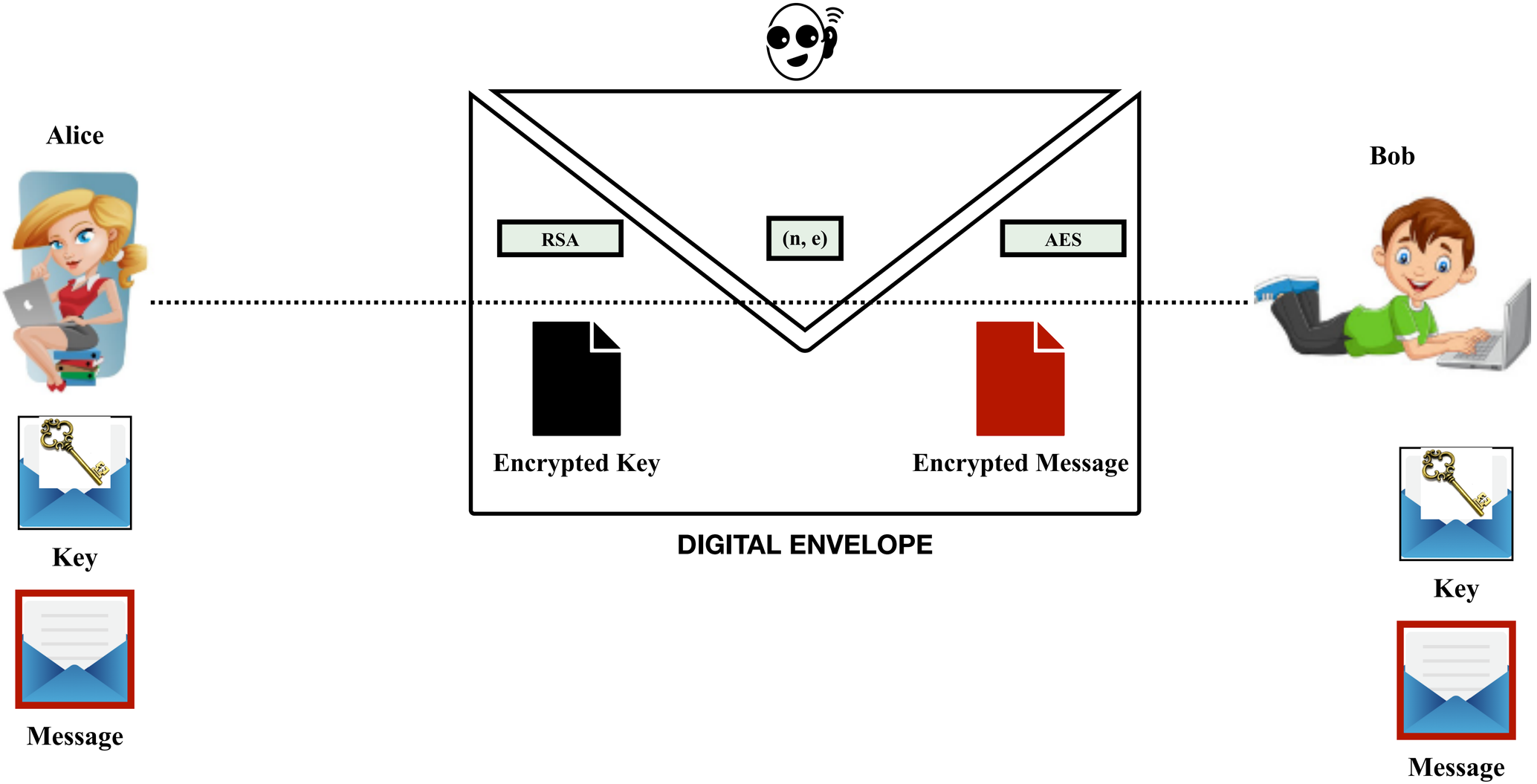
Exchanging Symmetric-key Material



Invoking Symmetric-Key Encryption



Digital Envelope



What is Inside?

- A digital envelope employs a two-layered encryption system for enhanced security:

    1. Symmetric key, &
    2. Public key encryption.

- This secure form of communication is crucial in today's digital age due to the ever-increasing threat of cyber attacks, hacking, and data breaches.
- It ensures that confidential data remains inaccessible to unauthorized individuals, safeguarding *privacy* and maintaining *data integrity*.

Application

1. **Secure file transfer**,
2. **Secure Email Communication,**
3. **Safeguarding communications** in distributed systems,
4. **E-commerce Transactions:** In online shopping, digital envelopes play an important role in protecting transaction data, such as credit card and personal information.

Email Encryption

- The most popular email encryption protocol is Pretty Good Privacy (PGP) which employs digital envelopes to ensure that only intended recipients can decrypt and read the message.

Demonstration

- Live demonstration of the key generation, encryption, and decryption processes.
- Highlights the security features of the implemented digital envelope.

Conclusion

- Encrypted the file of 100 Mb from RSA only.
- In contrast to this,
  - First encrypted 256-bit key using RSA encryption and shared it the recipient.
  - Recipient decrypted it using the RSA Decryption.
  - Then we encrypted the file with AES using AES and the pre-shared key of length 256 bit.
- Observed a huge time-difference for the file 100 Mb.
- Achieved a balance between security and efficiency by combined use of AES & RSA.
- Insights into modern cryptographic protocols for real-world applications.


THANK
YOU!