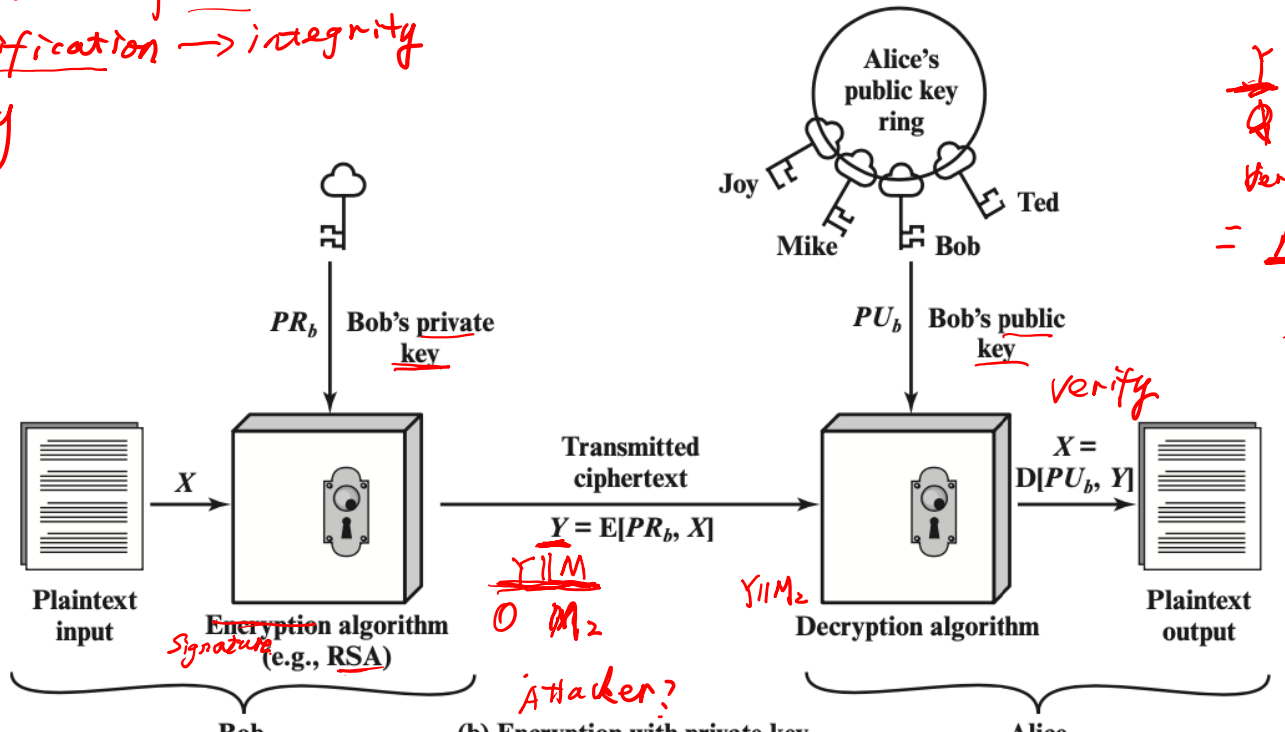
Public-Key Encryption: Definition

- Three parts:
  - KeyGen() → *PK*, *SK*: Generate a public/private keypair, where *PK* is the public key, and *SK* is the private (secret) key
  - Enc(*PK*, *M*) → *C*: Encrypt a plaintext *M* using public key *PK* to produce ciphertext *C*
  - Dec(*SK*, *C*) → *M*: Decrypt a ciphertext *C* using secret key *SK*
- Properties
  - **Correctness**: Decrypting a ciphertext should result in the message that was originally encrypted
    - Dec(*SK*, Enc(*PK*, *M*)) = *M* for all *PK*, *SK* ← KeyGen() and *M*
  - **Efficiency**: Encryption/decryption should be fast
  - **Security**: 1. Alice (the challenger) just gives Eve (the adversary) the public key, and Eve doesn't request encryptions. Eve cannot guess out anything; 2. computationally infeasible to recover M with PK and ciphertext

Public-Key Cryptography - Signature

Motivation:
1. prove source or id of doc
2. detect modification → integrity

Confidentiality



verify

Y || M
Verify [PK, Y]
= M'
M' ≠ M
if Yes, No modification
else, attack.

Source?
(SK, PK) ✓
only owned by Bob

Signature

Y || M
or M2

Y || M2

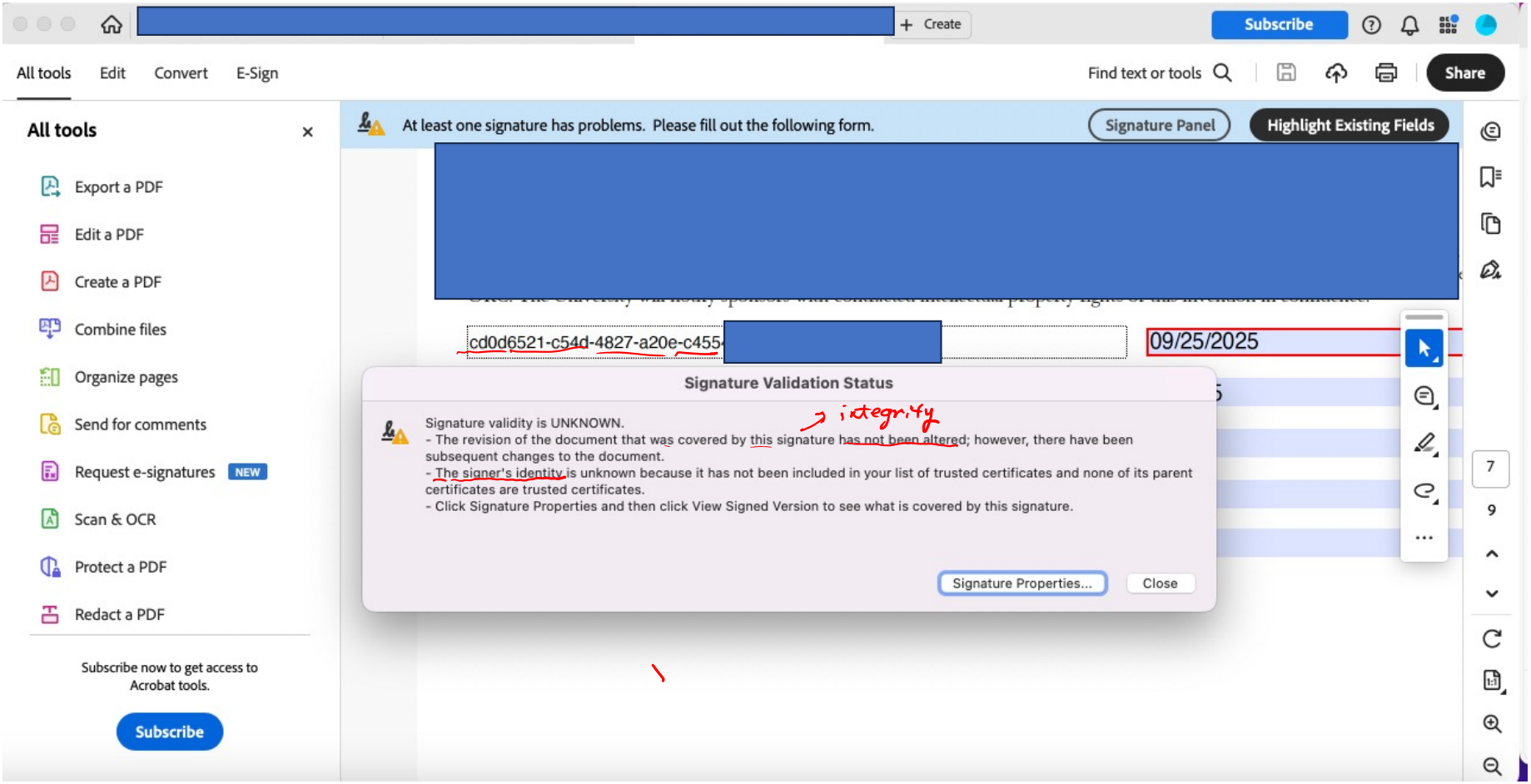
Attacker?

$M_2 \neq M'$

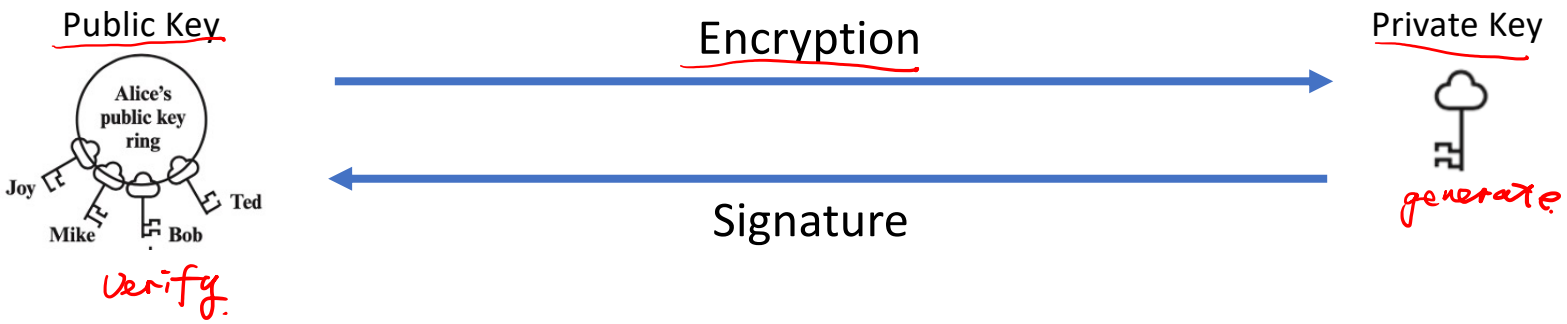
Send

② Y? SK X

③ $Y_2 \| M_2$ ← $SK_{attacker}$ Man-in-middle attack


Create
Subscribe
All tools
Edit
Convert
E-Sign
Find text or tools
Share
All tools
Export a PDF
Edit a PDF
Create a PDF
Combine files
Organize pages
Send for comments
Request e-signatures
NEW
Scan & OCR
Protect a PDF
Redact a PDF
Subscribe now to get access to Acrobat tools.
Subscribe
At least one signature has problems. Please fill out the following form.
Signature Panel
Highlight Existing Fields
cd0d6521-c54d-4827-a20e-c455
09/25/2025
Signature Validation Status
integrity
Signature validity is UNKNOWN.
- The revision of the document that was covered by this signature has not been altered; however, there have been subsequent changes to the document.
- The signer's identity is unknown because it has not been included in your list of trusted certificates and none of its parent certificates are trusted certificates.
- Click Signature Properties and then click View Signed Version to see what is covered by this signature.
Signature Properties...
Close
7
9

Review


Public Key
Alice's public key ring
Joy
Ted
Mike
Bob
verify
Encryption
Signature
Private Key
generate

Public-Key application

- can classify uses into 3 categories:
  - **encryption/decryption** (provide secrecy)
  - **digital signatures** (provide authentication)
  - **key exchange** (of session keys)
- some algorithms are suitable for all uses; others are specific to one
- Either of the two related keys can be used for encryption, with the other used for decryption

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie–Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic curve	Yes	Yes	Yes

TLS 1.2 – Use Public Key for Session Key Exchange

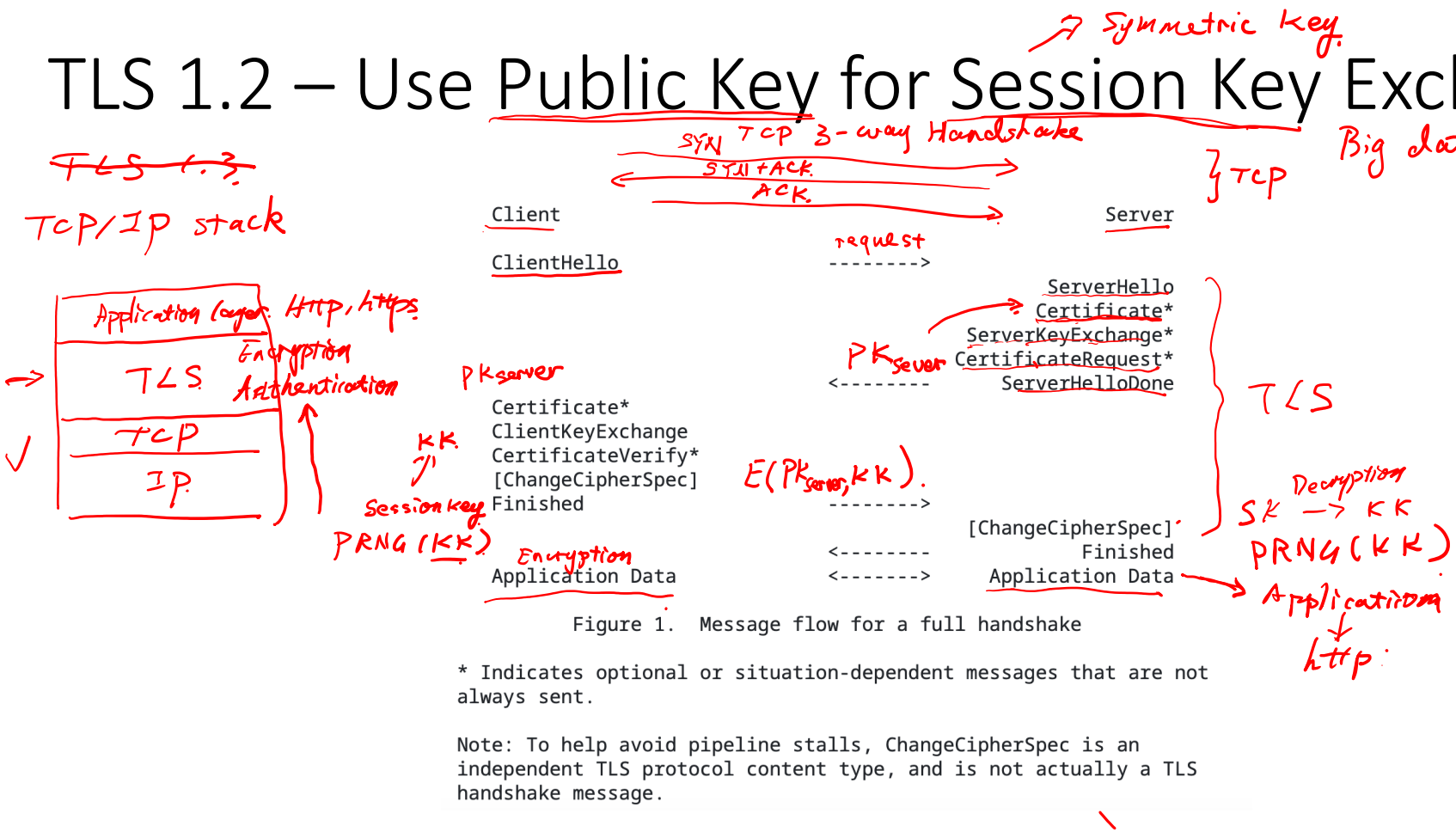


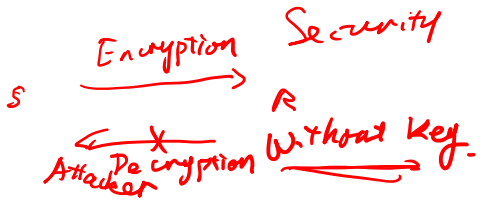
Figure 1. Message flow for a full handshake

* Indicates optional or situation-dependent messages that are not always sent.

Note: To help avoid pipeline stalls, ChangeCipherSpec is an independent TLS protocol content type, and is not actually a TLS handshake message.

RFC 5246: The Transport Layer Security (TLS) Protocol - Version 1.2

Security of Public Key Schemes



- Keys used are very large (>512bits) 4096 bits
  - like private key schemes brute force **exhaustive search** attack is always theoretically possible
- Security relies on a large enough difference in difficulty between easy (en/decrypt) and hard (cryptanalyze) problems
  - more generally the hard problem is known, it's just made too hard to do in practice

p · q → prime

- Requires the use of very large numbers, hence is slow compared to private/symmetric key schemes