Pretty Good Privacy (PGP)

19CSE311 Computer Security
Jevitha KP
Department of CSE

Pretty Good Privacy (PGP)

- PGP was invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e.,
  - privacy,
  - integrity,
  - authentication, and
  - non-repudiation in the sending of email.

Pretty Good Privacy (PGP)

- PGP uses a **digital signature** to provide integrity, authentication, and non-repudiation.

- PGP uses a **combination of secret key encryption and public key encryption** to provide **privacy**.

- PGP provides **authentication** through the use of Digital Signature.

- It provides **confidentiality** through the use of **symmetric block encryption.**

Pretty Good Privacy (PGP)

- PGP is an open source and freely available software package for email security.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

PGP to create secure e-mail

- The e-mail message is **hashed by using a hashing function** to create a **digest**.

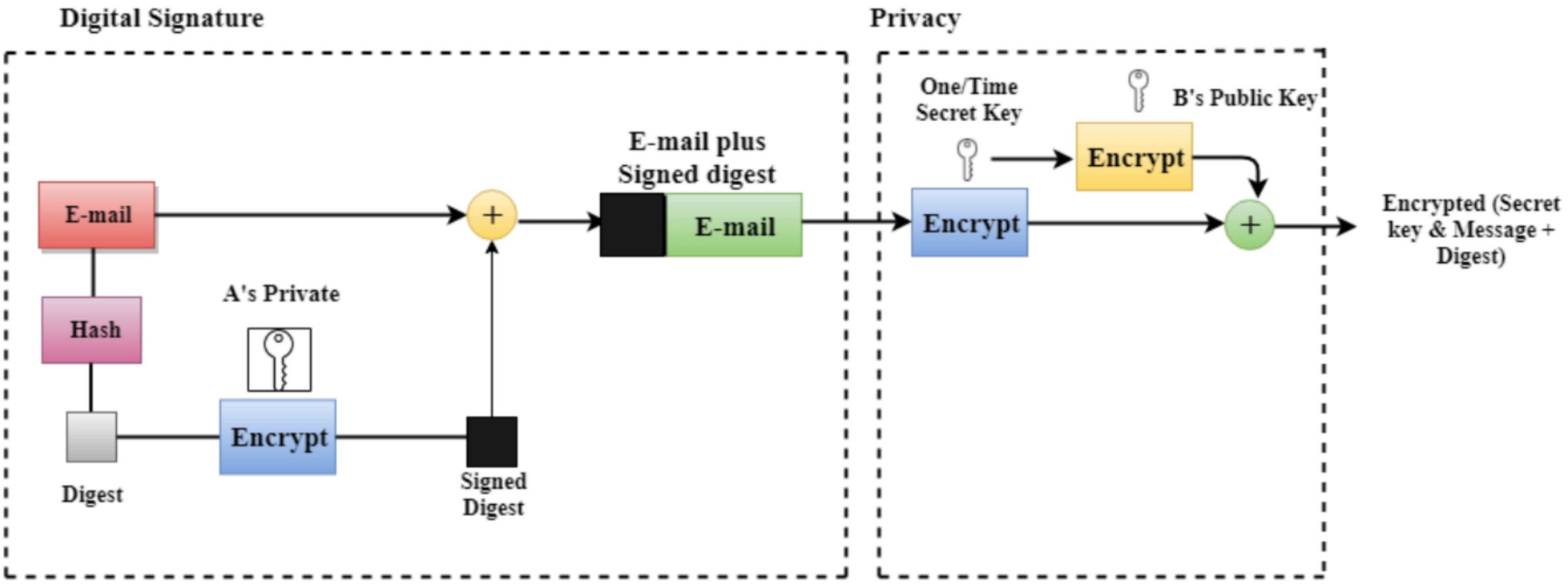
- The digest is then **encrypted** to form a **signed digest** by using the **sender's private key**, and then signed digest is added to the original email message.

- The original message and signed digest are encrypted by using a **one-time secret key** created by the sender.

- The secret key is encrypted by using a receiver's public key.

- Both the encrypted secret key and the encrypted combination of message and digest are sent together.

PGP At Sender site



PGP uses hashing and a combination of three keys to generate the original message

- The receiver receives the combination of **encrypted secret key** and **message digest** is received.

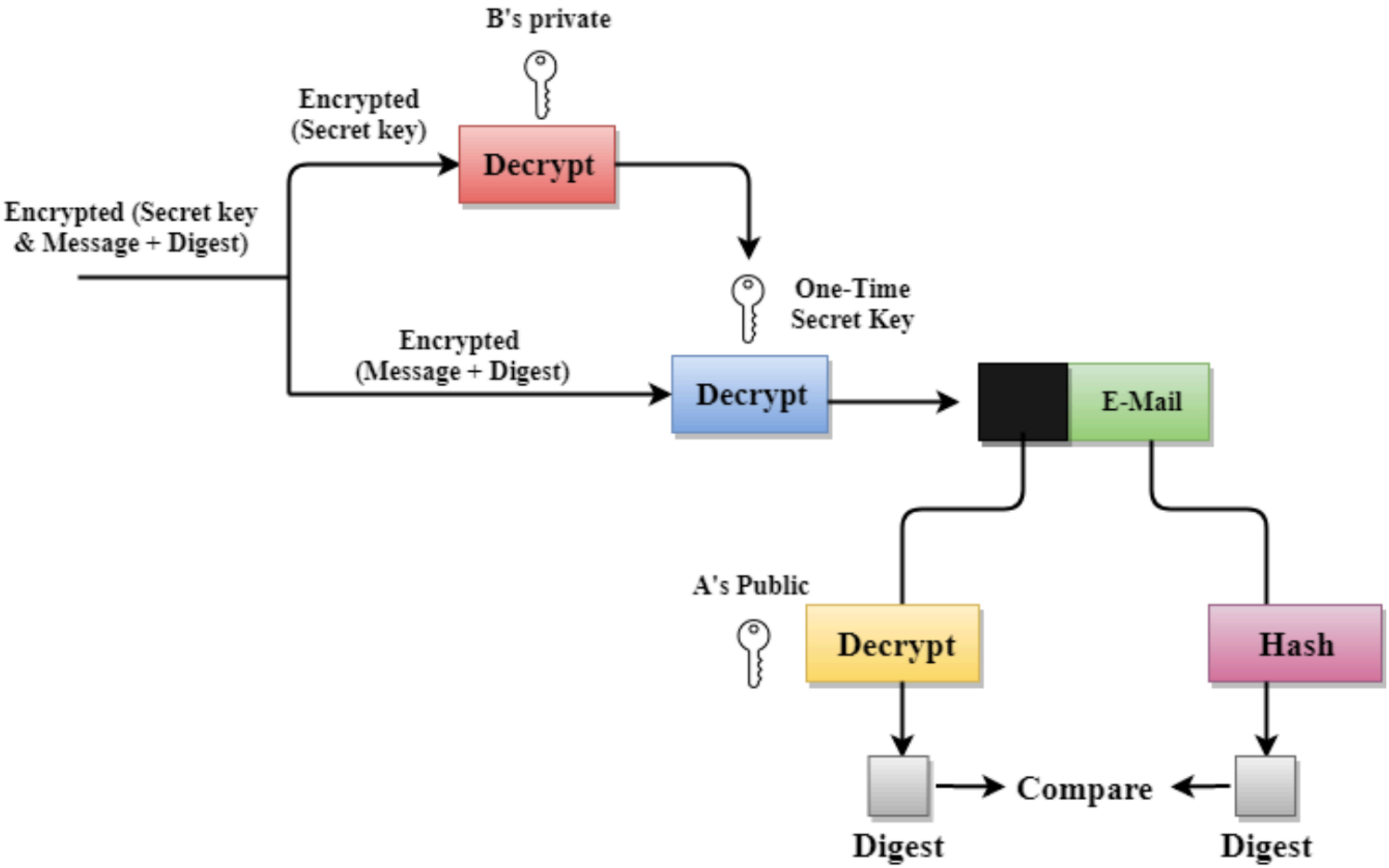
- The encrypted secret key is **decrypted** by using the **receiver's private key to get the one-time secret key.**

- The secret key is then used to **decrypt the combination of message and digest.**

- The digest is **decrypted by using the sender's public key,** and the original message is hashed by using a hash function to create a digest.

- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at Receiver site B



Public-Key Algorithms

- The public-key algorithms that are used for signing the digests or encrypting the messages :

ID	*Description*
1	RSA (encryption or signing)
2	RSA (for encryption only)
3	RSA (for signing only)
16	ElGamal (encryption only)
17	DSS
18	Reserved for elliptic curve
19	Reserved for ECDSA
20	ElGamal (for encryption or signing)
21	Reserved for Diffie-Hellman
100–110	Private algorithms

Symmetric-Key Algorithms

ID	*Description*
0	No Encryption
1	IDEA
2	Triple DES
3	CAST-128
4	Blowfish
5	SAFER-SK128
6	Reserved for DES/SK
7	Reserved for AES-128
8	Reserved for AES-192
9	Reserved for AES-256
100–110	Private algorithms

Hash Algorithms

ID	*Description*
1	MD5
2	SHA-1
3	RIPE-MD/160
4	Reserved for double-width SHA
5	MD2
6	TIGER/192
7	Reserved for HAVAL
100–110	Private algorithms

Compression Algorithms

ID	*Description*
0	Uncompressed
1	ZIP
2	ZLIP
100–110	Private methods

PGP Certificates

- PGP uses certificates to authenticate public keys.
- However, the process is totally different.
- In X.509, there is a single path from the fully trusted authority to any certificate
- In PGP, there can be multiple paths from fully or partially trusted authorities to any subject.

Disadvantages of PGP Encryption

- The Administration is difficult:
    - The different versions of PGP complicate the administration.
- Compatibility issues:
    - Both the sender and the receiver must have compatible versions of PGP.
    - For example, if you encrypt an email by using PGP with one of the encryption technique, the receiver has a different version of PGP which cannot read the data.

Disadvantages of PGP Encryption

- Complexity:
    - PGP is a complex technique.
    - Other security schemes use symmetric encryption that uses one key or asymmetric encryption that uses two different keys.
    - PGP uses a hybrid approach that implements symmetric encryption with two keys.
    - PGP is more complex, and it is less familiar than the traditional symmetric or asymmetric methods.

Disadvantages of PGP Encryption

- No Recovery:
    - Computer administrators face the problems of losing their passwords.
    - In such situations, an administrator should use a special program to retrieve passwords.
    - However, PGP does not offer such a special program for recovery;
    - encryption methods are very strong so, it does not retrieve the forgotten passwords results in lost messages or lost files.