Email Communication Encryption Protocol

This document outlines a sample protocol for encrypting email communications to ensure confidentiality, authenticity, and integrity.

1. Objectives

- Confidentiality: Prevent unauthorized reading of email content.
- Integrity: Ensure email contents are not altered in transit.
- Authentication: Confirm sender identity.

2. Protocol Overview

1. Key Exchange
2. Message Encryption
3. Digital Signing
4. Email Transmission
5. Decryption & Verification

3. Key Exchange

- Each participant generates their own public/private key pair (e.g., RSA 2048-bit).
- Public keys are distributed, e.g., via a public directory or direct exchange.

4. Message Encryption & Signing

1. A random symmetric session key is generated (e.g., AES-256).
2. The email message is encrypted with the session key.
3. The session key is encrypted with the recipient's public key.
4. The encrypted message digest (hash) is signed with the sender's private key.

5. Email Structure Sample

```
-----BEGIN ENCRYPTED EMAIL-----
Encrypted-Session-Key: [Base64]
Encrypted-Message: [Base64]
Signature: [Base64]
-----END ENCRYPTED EMAIL-----
```

6. Email Transmission

- Send the structured encrypted email to the recipient via SMTP or another protocol.

7. Decryption & Verification

1. Recipient decrypts the session key with their private key.
2. Uses the session key to decrypt the message.
3. Validates the digital signature using the sender's public key.

8. Algorithm Reference Table

Purpose	Algorithm Example
Asymmetric Encryption	RSA, ECC
Symmetric Encryption	AES-256
Hashing	SHA-256
Digital Signature	RSA, ECDSA

9. Notes

- Replace algorithm choices based on organizational security requirements.
- Regularly update and manage keys securely.
- Ensure compliance with relevant cybersecurity standards.