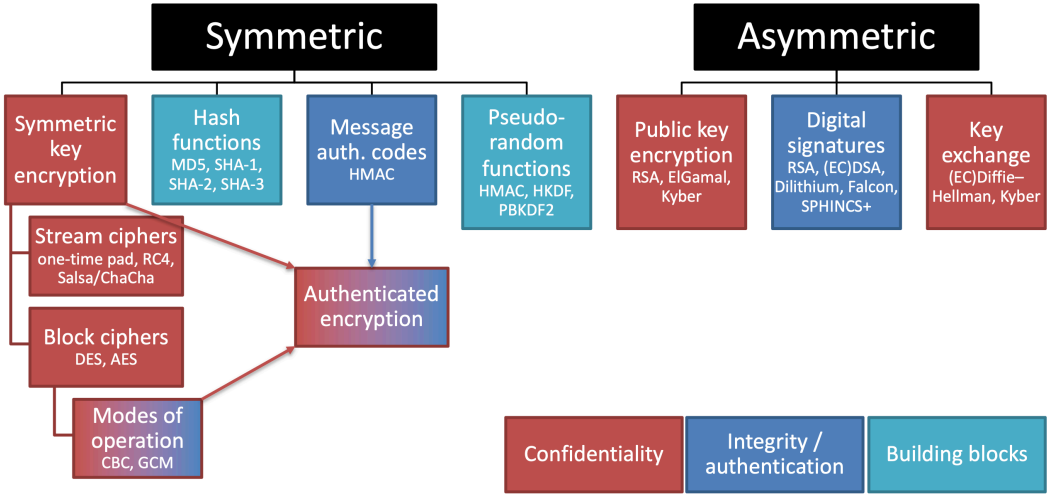
# Topic 4.0
# Applications

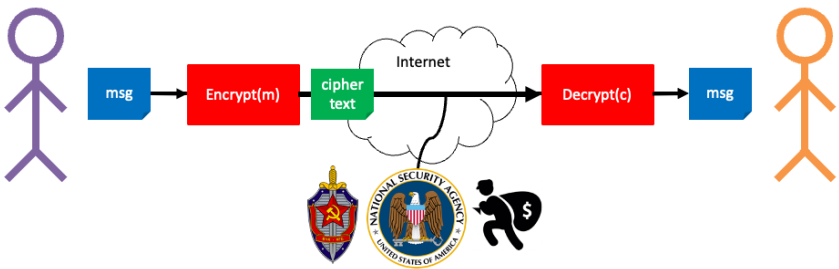
Douglas Stebila

CO 487/687: Applied Cryptography
Fall 2024

# Map of cryptographic primitives

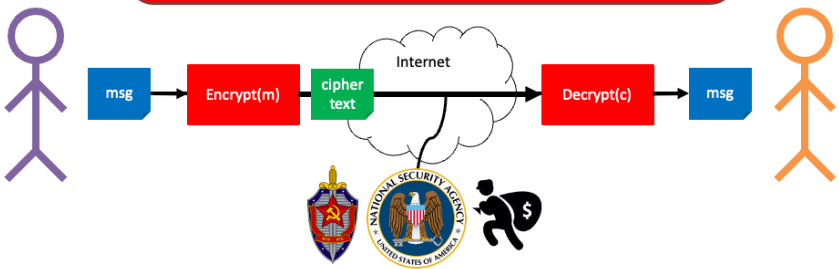


# Encryption using a secret function

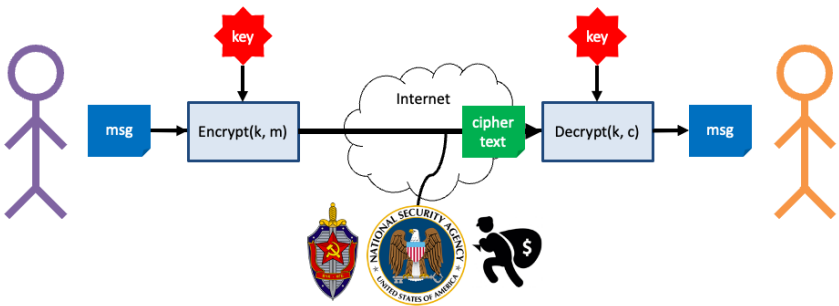


# Encryption using a secret function

Relying on a secret function violates Kerckhoff's principle of avoiding security by obscurity



# Symmetric encryption



## Man-in-the-middle (MITM) attack on symmetric encryption:

### What if an active adversary modifies transmissions?

# Authenticated encryption

# Authenticated encryption

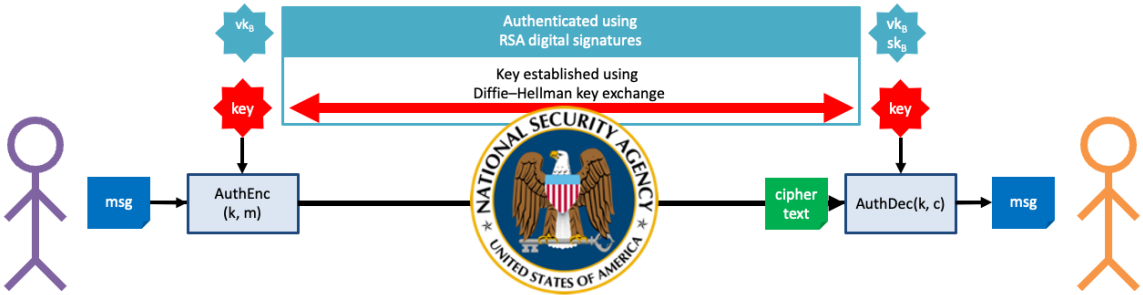
# Key exchange + authenticated encryption

# Man-in-the-middle attack on key exchange:

## What if an active adversary impersonates Alice and Bob to each other?

# Building a secure channel: attempt 5

## Authenticated key exchange + authenticated encryption

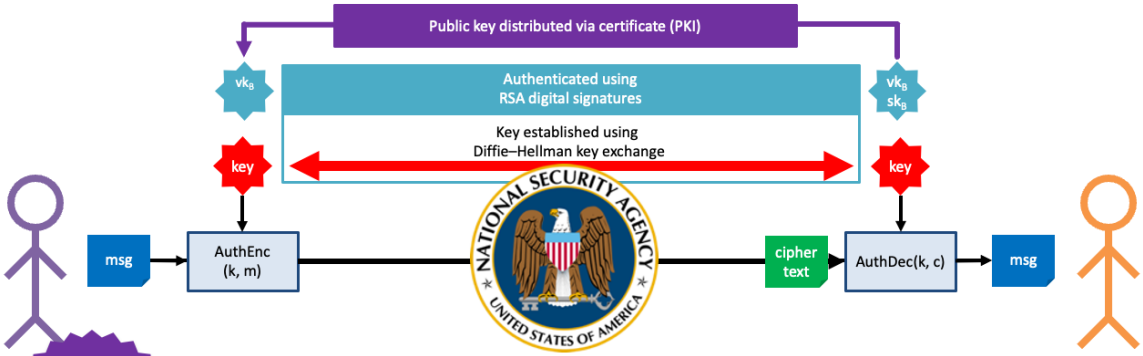


# Man-in-the-middle attack on authenticated key exchange

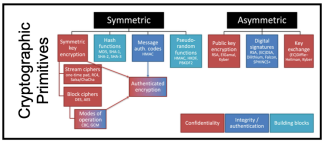
## What if an active adversary replaces Alice's public key?

# Building a secure channel: attempt 6

## Certified authenticated key exchange + authenticated encryption



# Applications




| Key management | Secure channels | Other applications |
|---|---|---|
| • PKI<br>• X.509 certificates | • TLS<br>• SSH<br>• Signal | • Bitcoin<br>• Zero knowledge |

## Secure channels