

# Storage on an **insecure** medium

## ➔ Threat 1: **Loss**

Cryptography cannot be used to prevent loss. It may be used to yield loss. E.g ransomware

## ➔ Threat 2 & 3: **Disclosure & Theft**

Encrypted data at rest cannot be meaningfully disclosed or utilized without decryption. E.g PGP Whole Disk Encryption

## ➔ Threat 4: **Modification**

Cryptography can be used to verify the integrity of data at rest

# Definitions of a cryptosystem