Chapter 1 – Hide the Wish-Lists

"I don't want my roommate to see my gift."

ndhy

July 2, 2025

Secrets need Shelter.

Outline

1. Raw JSON $\rightarrow$ unreadable data — the need for secrecy
2. Symmetric-encryption (AES-GCM, nonce, tag) — fast bulk confidentiality
3. The key hand-off problem — motivation for the next chapter
4. Activity: encrypt and decrypt wish-lists with a shared key

Can you read this?

```
{
  "item": "iPhone 15 Pro Max",
  "price": 799.99,
  "qty": 1
}
```

Can you read this?

```
{
  "item": "iPhone 15 Pro Max",
  "price": 799.99,
  "qty": 1
}
```

Challenge
Turn it into nonsense in $<$ **100 ms**.

Plaintext → Ciphertext in 80 ms

```
$ echo '{"item": "iPhone 15 Pro Max","price": 799.99,"qty": 1}' | \
  openssl enc -aes-256-cbc -nosalt -pbkdf2 -iter 10000 -k hunter2 | base64
3d2J0MtQmwNYIgZA1gjl2qQ2wofKkCbrBxhdI7p5Bvjv1Su5/kG42DOEr6D8g42eCxOM1EFTtDf
    +
zhpthhkv7A==
```

Plaintext → Ciphertext in 80 ms

```
$ echo '{"item": "iPhone 15 Pro Max","price": 799.99,"qty": 1}' | \
  openssl enc -aes-256-cbc -nosalt -pbkdf2 -iter 10000 -k hunter2 | base64
3d2J0MtQmwNYIgZA1gjl2qQ2wofKkCbrBxhdI7p5Bvjv1Su5/kG42DOEr6D8g42eCxOM1EFTtDf
    +
zhpthhkv7A==
```

- Instant visual proof that secrecy "works".
- The key ("`hunter2`") is everything.

One Key, Two Roles

- **Same** key locks & unlocks.
- Hardware speed: $\sim$GB/s.
- Perfect for laptops, backups, cloud blobs.

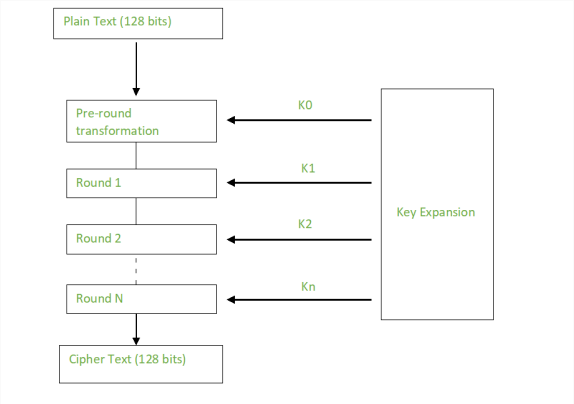

Figure 1: AES

AES-GCM in a Nutshell

Field	Size	Purpose
Nonce	96 bits	Unique label per packet
Ciphertext	*n* bytes	Scrambled content
Tag	128 bits	Integrity & authenticity

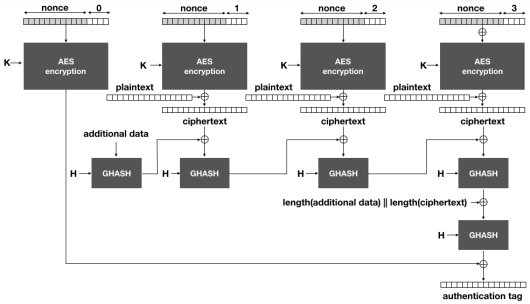

Figure 2: AES-GCM

Encryption is Useless Without the Key

Who hands the key to whom?
SMS? — Eavesdropped. Email? — Forwarded. USB? — Lost.

- One-roommate world $\rightarrow$ easy.
- Internet scale $\rightarrow$ the real headache.

Encrypt Your Lists

1. Partner creates a 32-byte key.
2. Each writes `wish.txt`, then:

```
openssl enc -aes-256-gcm -nosalt -k $KEY \
  -in wish.txt -out wish.enc -p -md md5
```

3. Exchange `wish.enc`, decrypt, compare checksums.
4. Match?

Debrief

Wins

- Blazing speed
- Integrity for free

Pains

- Sharing the key
- Nonce-reuse pitfall
- Human error

Key exchange comes next! **Public-Key Crypto**

Cheat-Sheet

- Encryption hides; *tags spot tampering*.
- AES-GCM = industry workhorse.
- Key distribution is the unsolved core — stay tuned.

Questions?