Hashing vs Encryption

Computing

One is reversible and one is not — and choosing wrong is a breach.

Hashing — one way

- Cannot be reversed, by design
- Same input always gives the same output
- Fixed-length output
- For passwords, integrity, deduplication
- SHA-256 for data, Argon2 for passwords

Encryption — two way

- Reversible with the key
- Same input can give different output (IV)
- For data you must read again
- At rest and in transit
- AES-GCM, ChaCha20-Poly1305

THE DIFFERENCE THAT MATTERS

Encoding is neither. Base64 provides no security at all — it is a transport format that anyone can reverse.

Encrypting a password instead of hashing it means one leaked key exposes every password at once.