Security Introduction
- Confidentiality, Integrity, Availability
- Authentication, Authorization, Accounting
- Hackers by hat
- Defense in Depth (layers)
- Least Privilege
- Separation of Duties
- Security by Design
- Security by Obscurity
- Security Controls

Encryption
- Symmetric Encryption
- Public Key Encryption
- Substitution ciphers
- Trapdoor Functions
- Encryption Weakness
- AES
- Key Exchange
- Hashes
- Salt
- Authentication
- Digital Signatures

You may be asked to...
- Define terms and explain the general ideas of topics.
- Write excel formulas.
- Explain how the CIA principles apply to a scenario.
- Describe a layered security system or identify the layers.
- Decode/Encode using a Caesar cipher with the key.
- Explain how keys are used to encrypt/decrypt a message.

Excel and Data Topics
- Relative cell addresses
- Absolute cell addresses
- Formulas
- Functions
- Filling values
- Mean, Median, Mode

Hashes

$h(pwd1)$ ⟶
$h(pwd2)$ ⟶ hash value
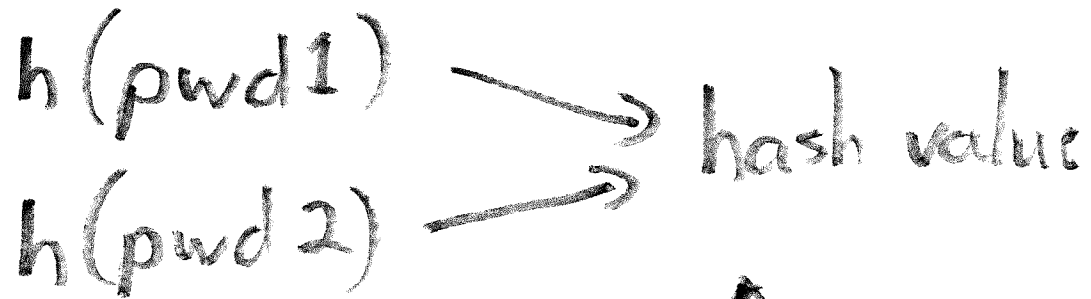
↑
collision:

either password
works

Ex-Meta employee files whistleblower suit for alleged security flaws at WhatsApp

Jonathan Vanian
α IN:JONATHAN-VANIAN-B704432/

WATCH LIVE

KEY POINTS

- A former Meta employee sued the company over allegations that its WhatsApp messaging service contained cybersecurity failures that could compromise user privacy.

- The former WhatsApp security head claimed he began receiving "negative performance feedback" shortly after his initial disclosure.

- A Meta spokesperson disputed Baig's allegations in a statement, and downplayed his role and ranking at the company.

What security principles?

During a test conducted with Meta's central security team, Baig alleged he "discovered that approximately 1,500 WhatsApp engineers had unrestricted access to user data, including sensitive personal information" and that the employees "could move or steal such data without detection or audit trail."

CIA

- Confidentiality
- Integrity
- Availability

AAA

- Authentication
- Authorization
- Accounting

Controls

- Physical
- Administrative
- Technical

Authentication factors

- You know
- You have
- You are

Layers

- Human
- Perimeter (physical)
- Network
- Endpoint (devices)
- Applications
- Data
- Assets

Hats

- Black -attackers
- White - defenders
- Grey – defense w/o permission
- Red – attacks attackers
- Blue - personal or hired
- Green - inexperienced

Principles

- Defense in Depth
- Least Privilege
- Separation of Duties
- Security by Design
- KISS
- (X) Security by Obscurity