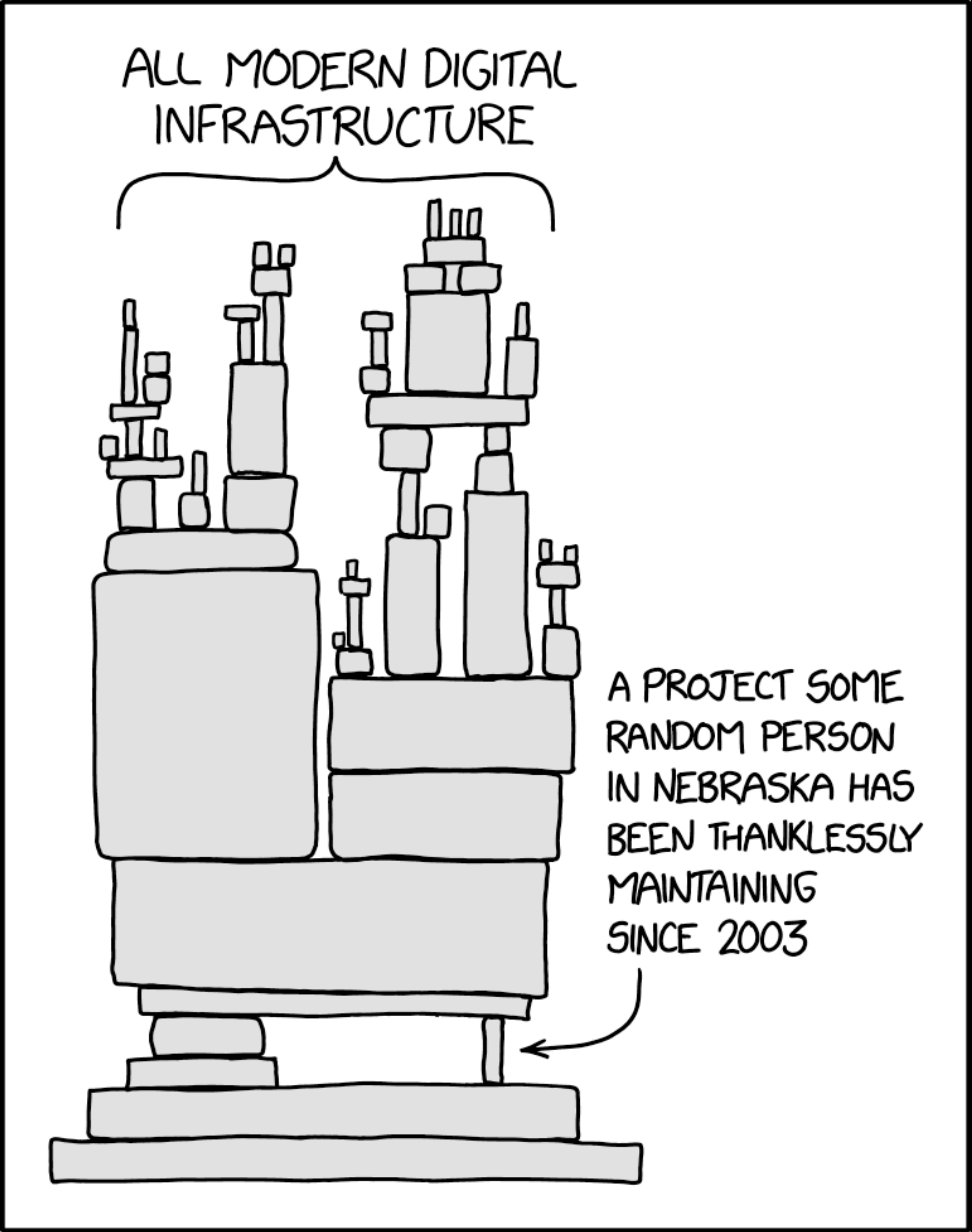
Practical Cryptographic Systems

Asymmetric Cryptography

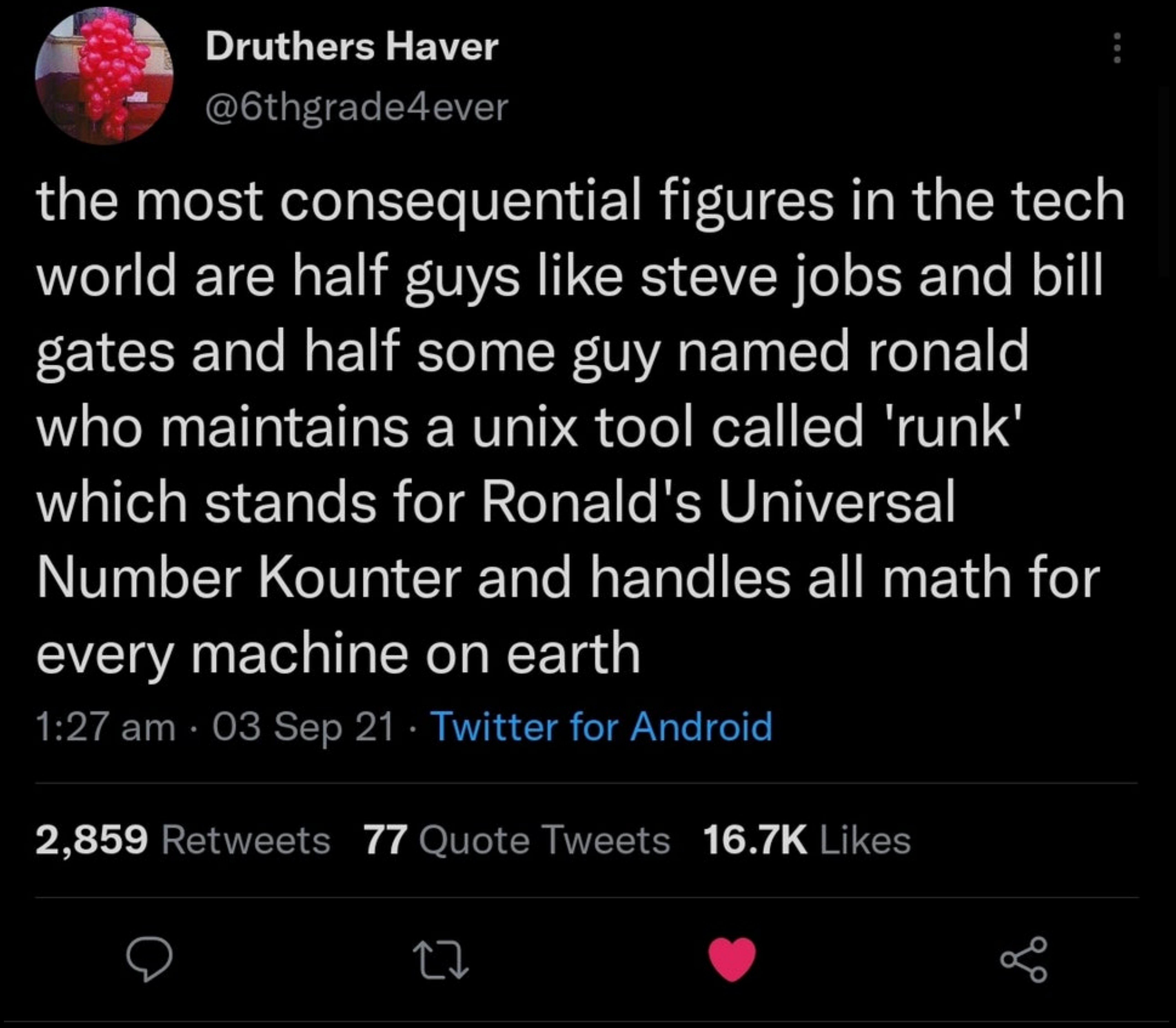
Some Housekeeping

- Office hours:
  - Monday (Alishah) 2-3:30
    Wednesday (Matt) 2-3:30
    Malone 307

News


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

https://imgs.xkcd.com/comics/dependency_2x.png

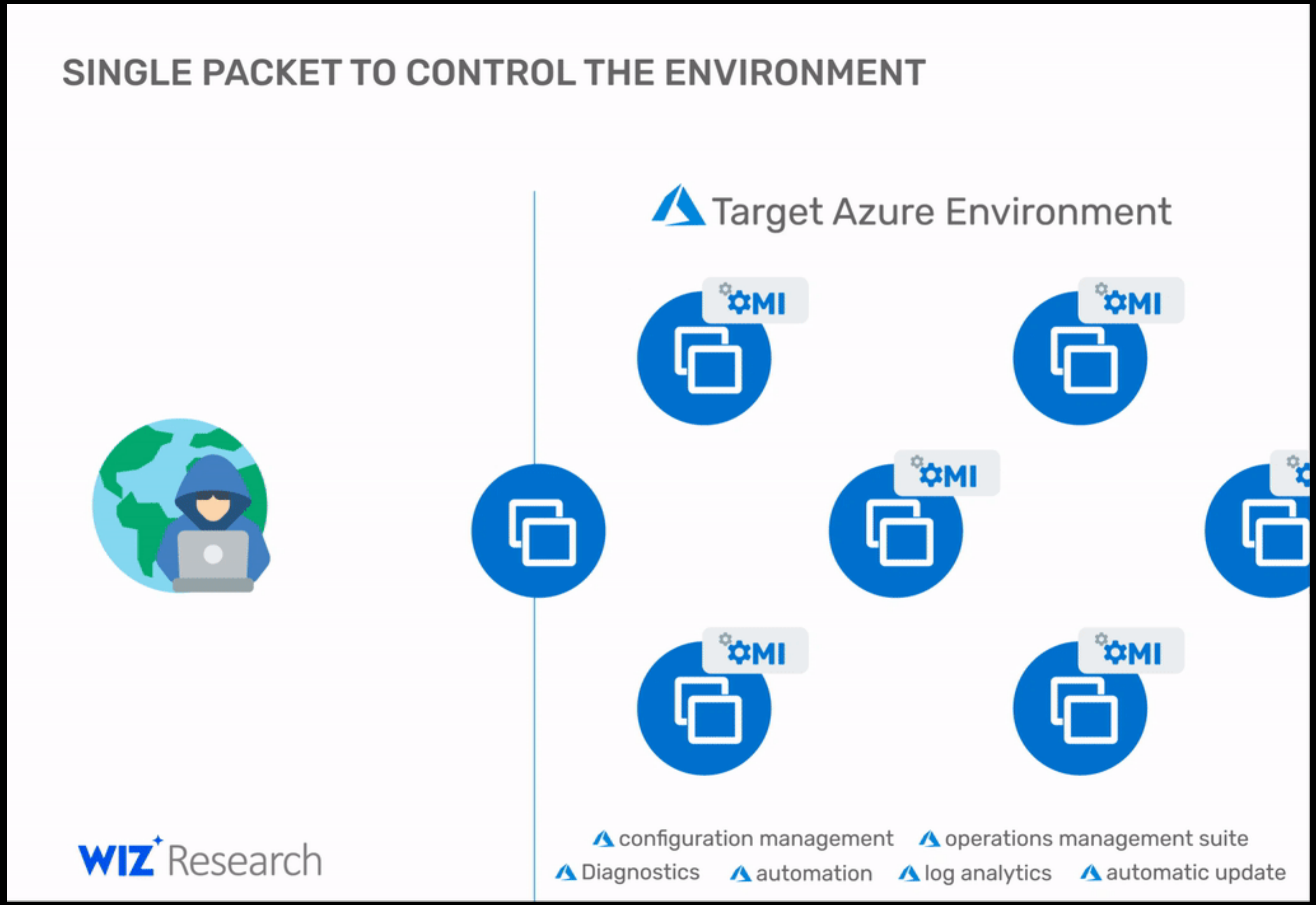


Druthers Haver
@6thgrade4ever

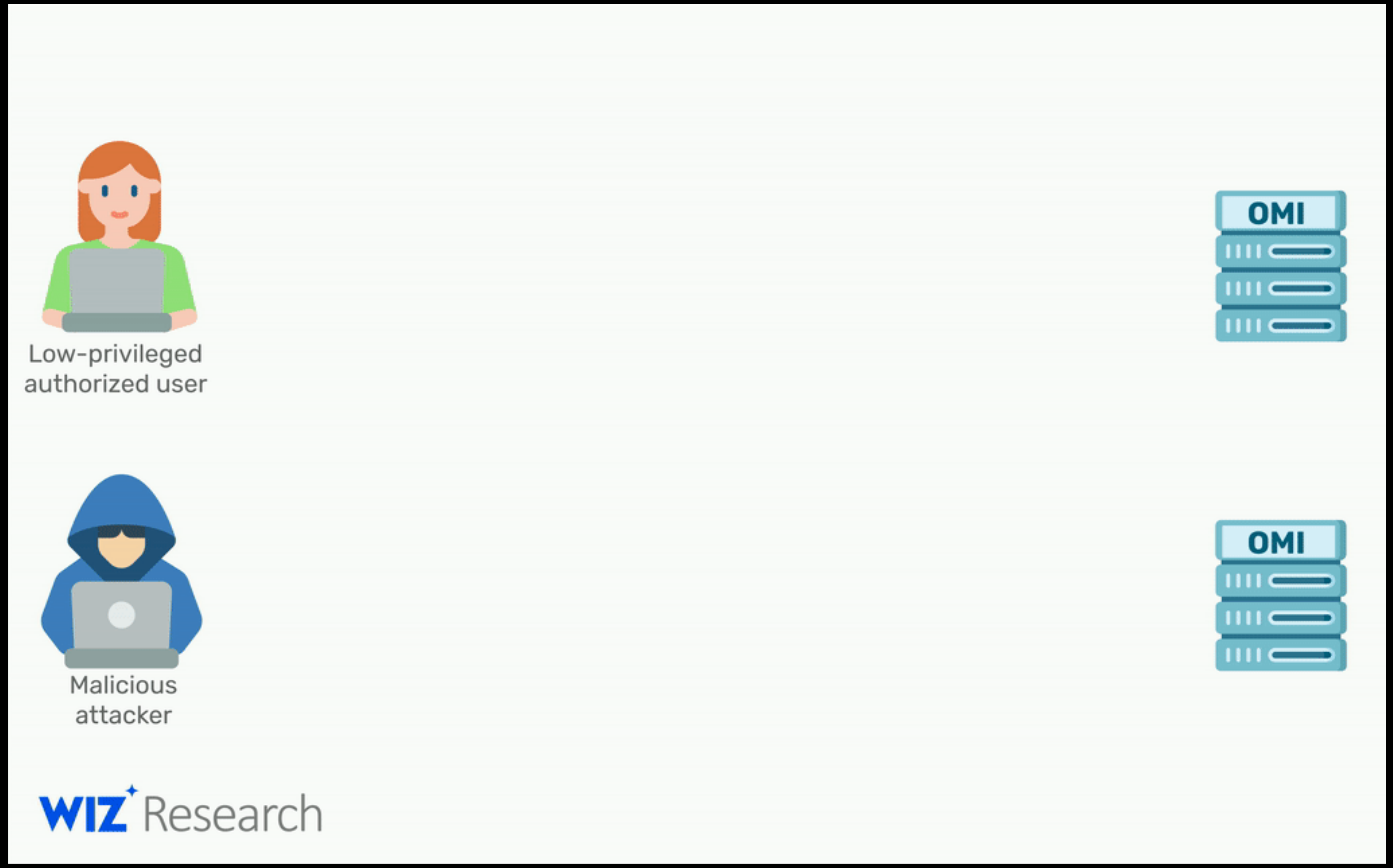
the most consequential figures in the tech world are half guys like steve jobs and bill gates and half some guy named ronald who maintains a unix tool called 'runk' which stands for Ronald's Universal Number Kounter and handles all math for every machine on earth

1:27 am · 03 Sep 21 · Twitter for Android

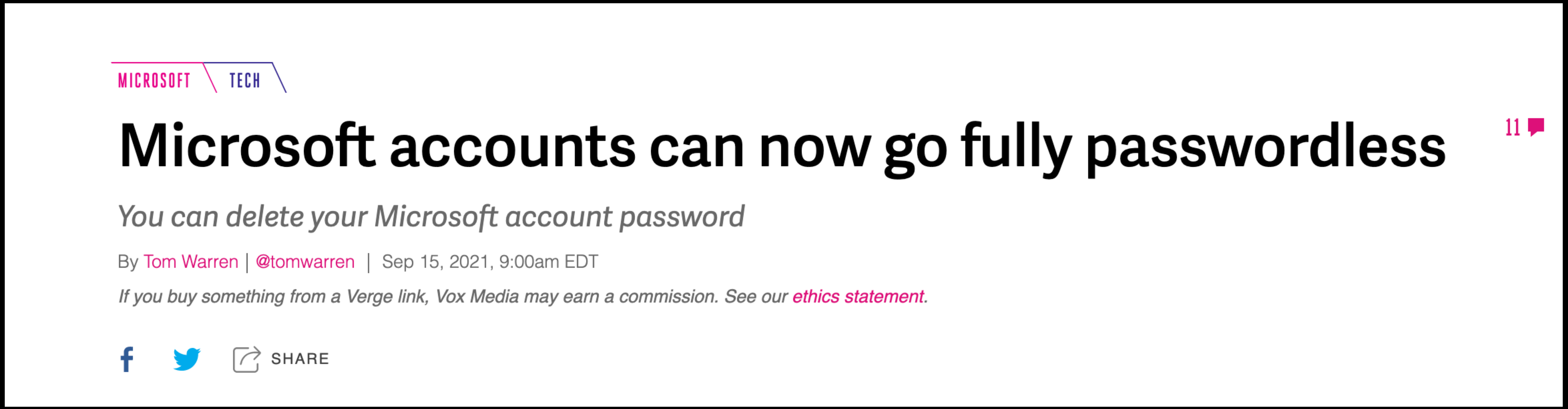
2,859 Retweets **77** Quote Tweets **16.7K** Likes



SINGLE PACKET TO CONTROL THE ENVIRONMENT



https://www.wiz.io/blog/secret-agent-exposes-azure-customers-to-unauthorized-code-execution



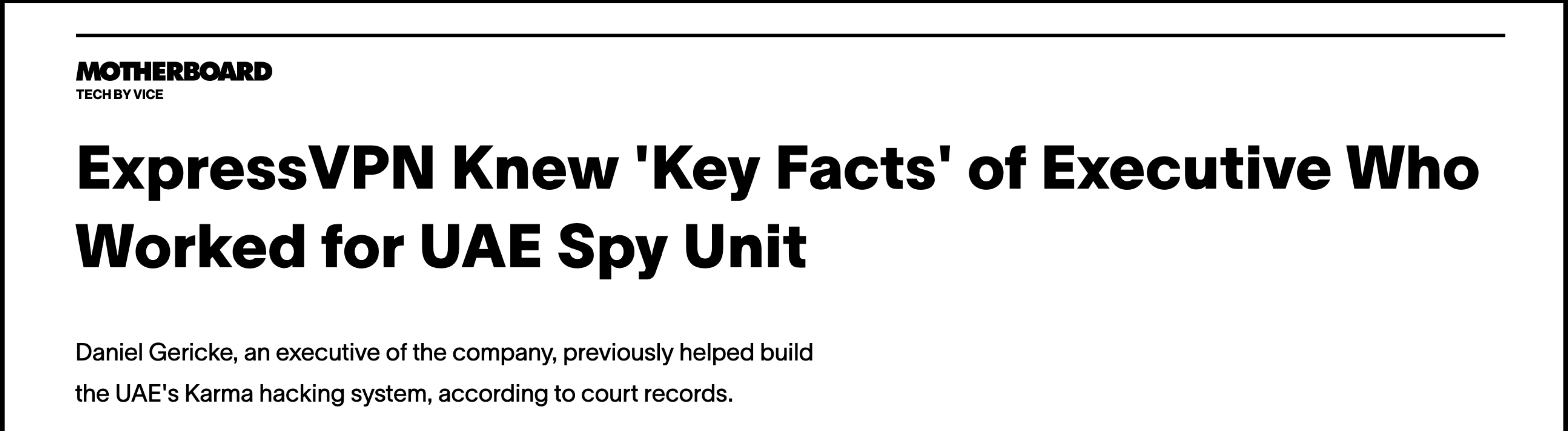
Microsoft accounts can now go fully passwordless

You can delete your Microsoft account password

By Tom Warren | @tomwarren | Sep 15, 2021, 9:00am EDT

If you buy something from a Verge link, Vox Media may earn a commission. See our ethics statement.

https://www.theverge.com/2021/9/15/22675175/microsoft-account-passwordless-no-password-security-feature



MOTHERBOARD
TECH BY VICE

ExpressVPN Knew 'Key Facts' of Executive Who Worked for UAE Spy Unit

Daniel Gericke, an executive of the company, previously helped build the UAE's Karma hacking system, according to court records.

https://www.vice.com/en/article/3aq9p5/expressvpn-uae-hacking-project-raven-daniel-gericke

MACs

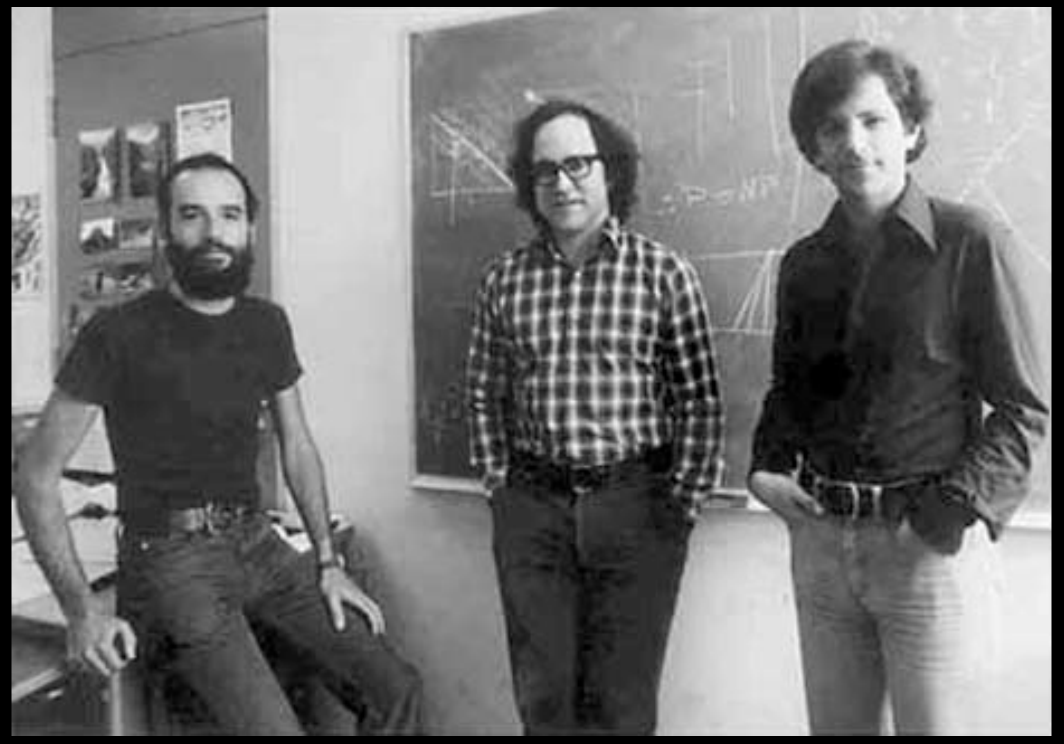
- Symmetric-key primitive
  - Given a key and a message, compute a “tag”
  - Tag can be verified using the same key
  - Any changes to the message detectable
- To prevent malleability:
  - Encrypt then MAC
  - Under separate keys

MACs

- Definitions of Security
    - Existential Unforgeability under CMA
- Examples:
    - HMAC (based on hash functions)
    - CMAC (block ciphers)

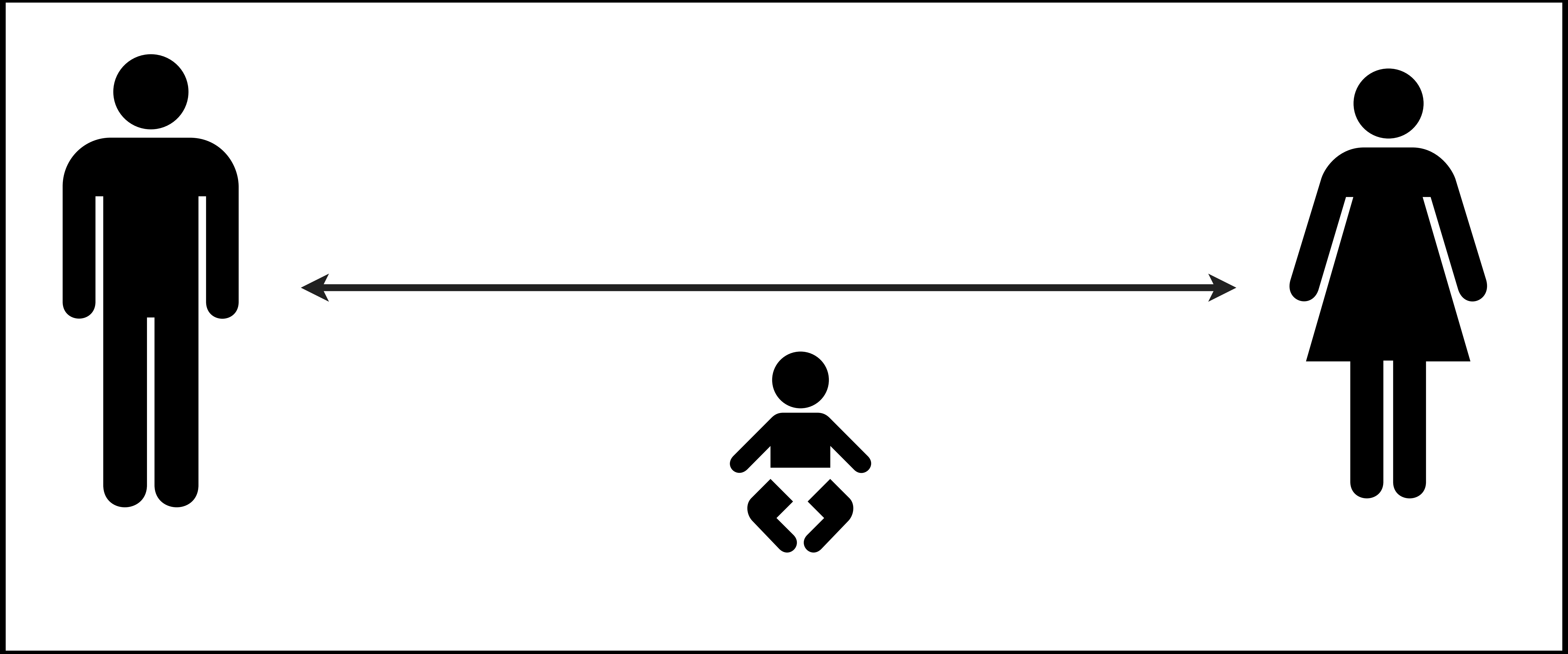
Asymmetric Crypto

- So far we've discussed symmetric crypto
  - Requires both parties to share a key
  - Key distribution is a hard problem!



Key Agreement

- Establish a shared key in the presence of a passive adversary

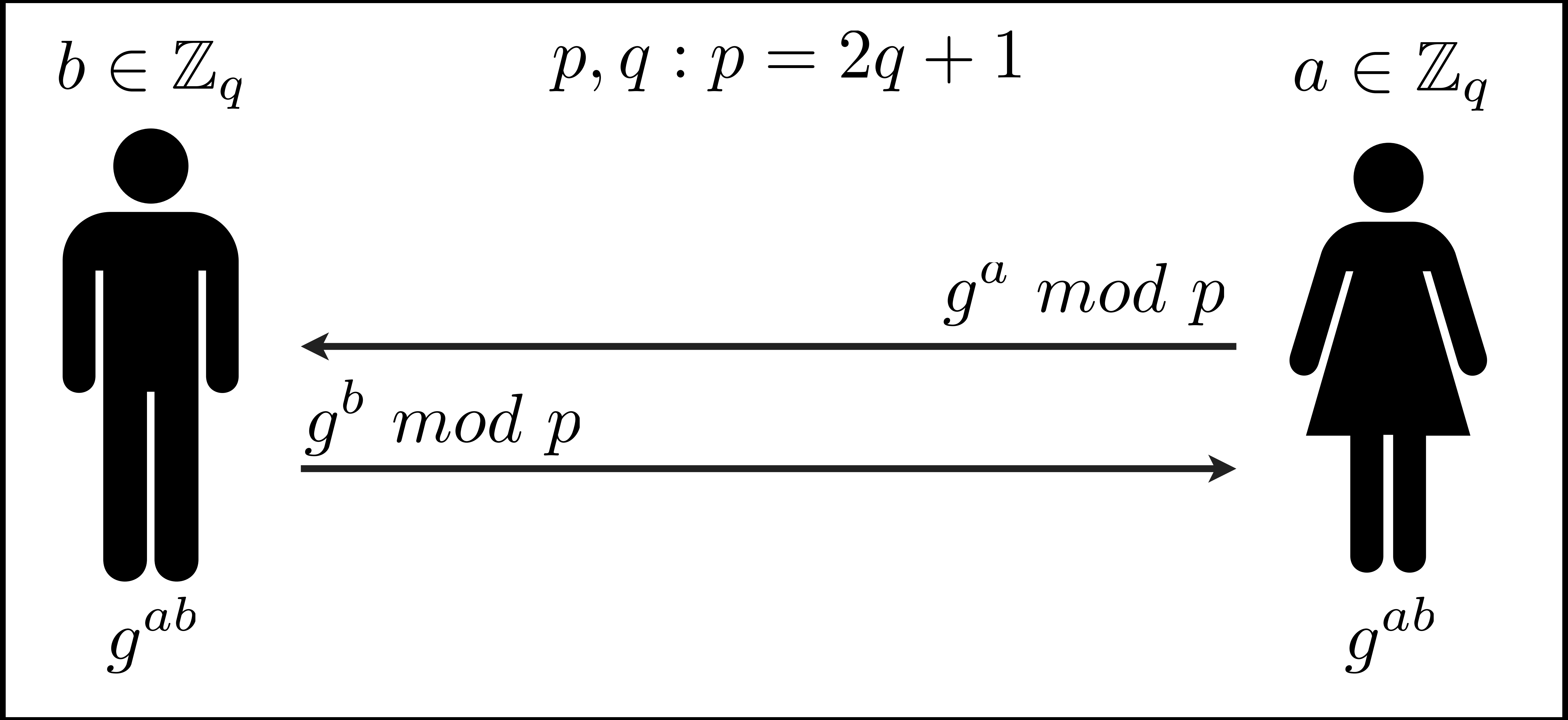


Lets Talk Groups

Malcolm Williamson in 72

Diffie-Hellman in 76

D-H Protocol



$p, q : p = 2q + 1$

$b \in \mathbb{Z}_q$

$a \in \mathbb{Z}_q$

$g^a \ mod \ p$

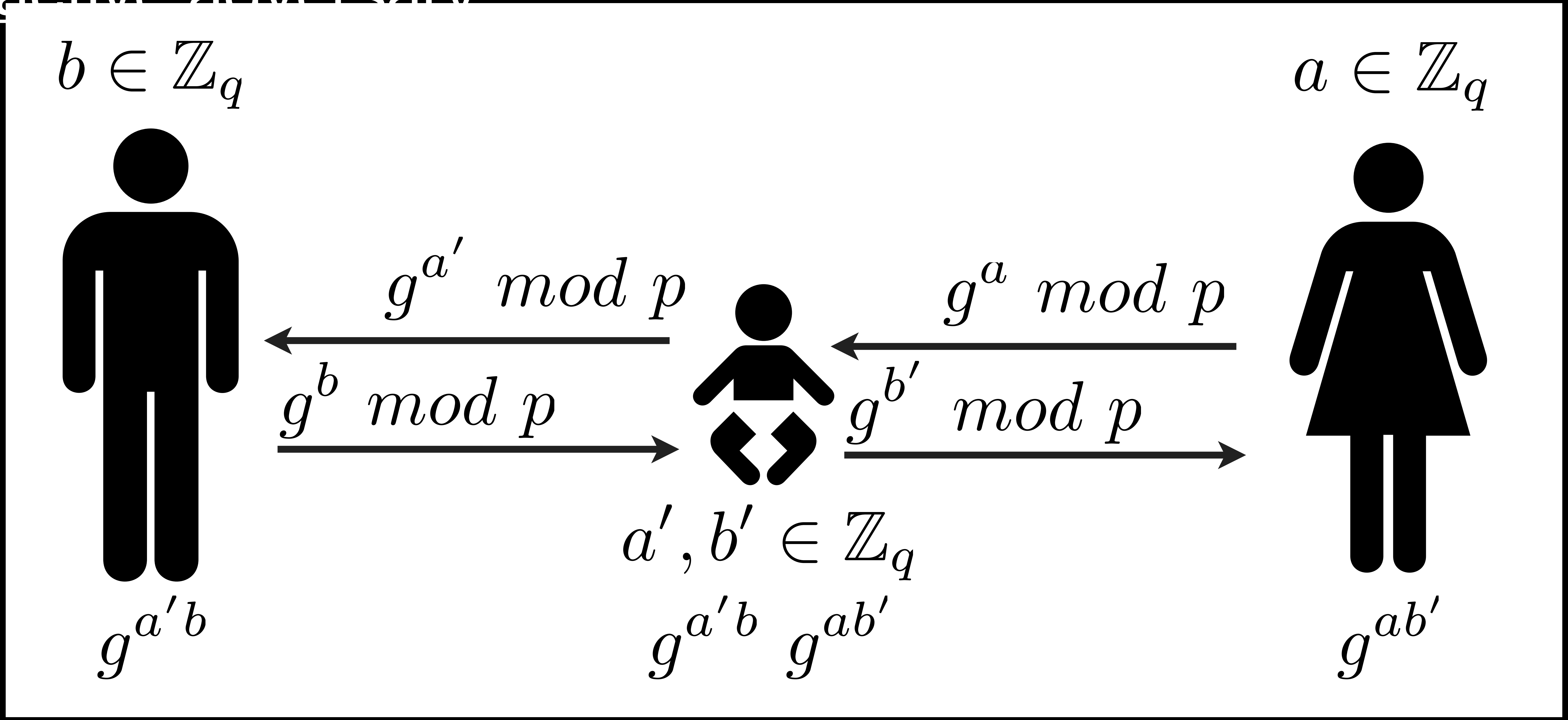
$g^b \ mod \ p$

g^{ab}

g^{ab}

Man in the Middle

- Assume an active adversary:

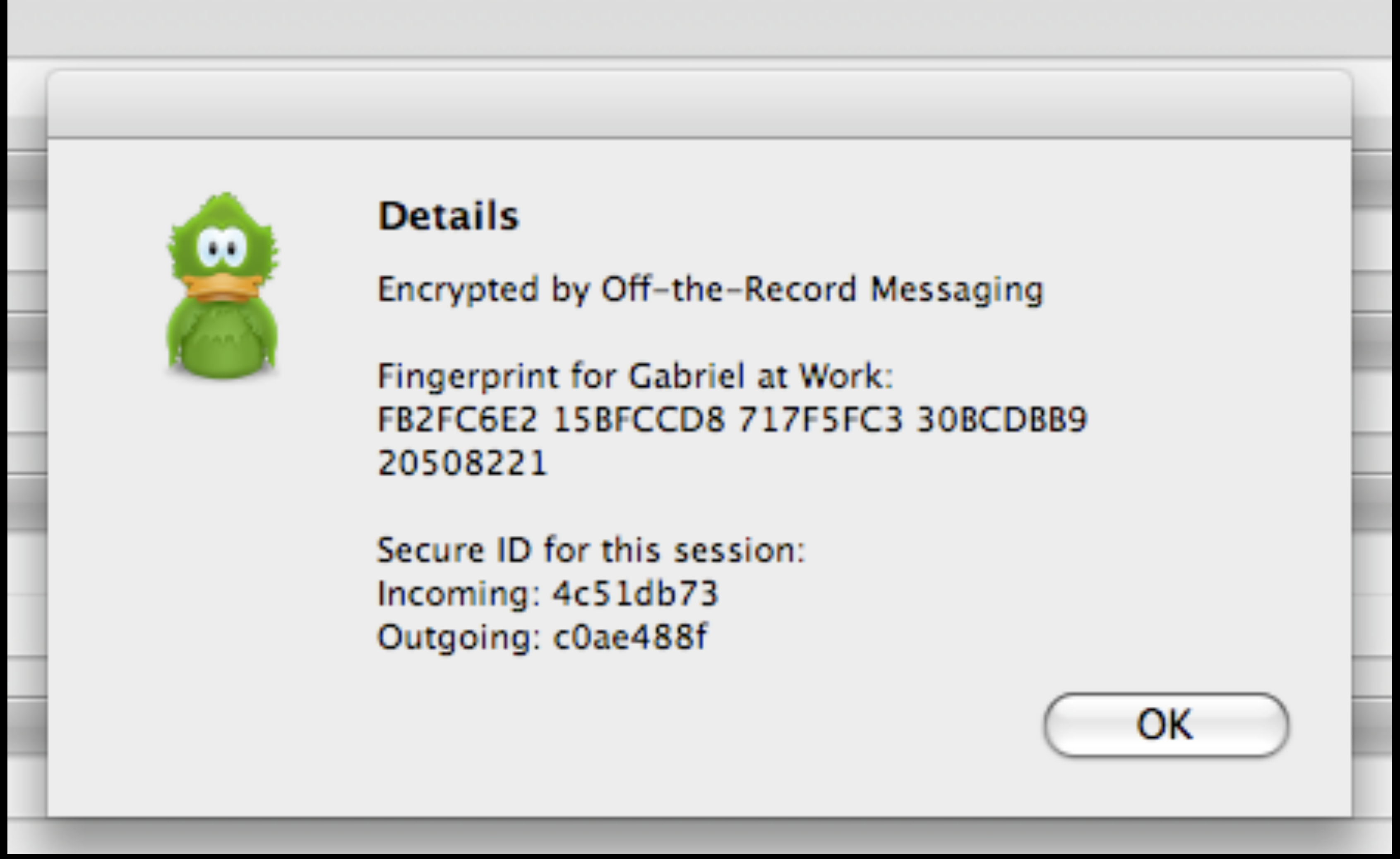


Man in the Middle

- Caused by lack of authentication
  - D-H lets us establish a shared key with anyone...
    but that’s the problem...
- Solution: Authenticate the remote party

Preventing MITM

- Verify key via separate channel
- Password-based authentication
- Authentication via PKI



Details

Encrypted by Off-the-Record Messaging

Fingerprint for Gabriel at Work:
FB2FC6E2 15BFCCD8 717F5FC3 30BCDBB9
20508221

Secure ID for this session:
Incoming: 4c51db73
Outgoing: c0ae488f

Next Time

- Mathematics of Public Key Background