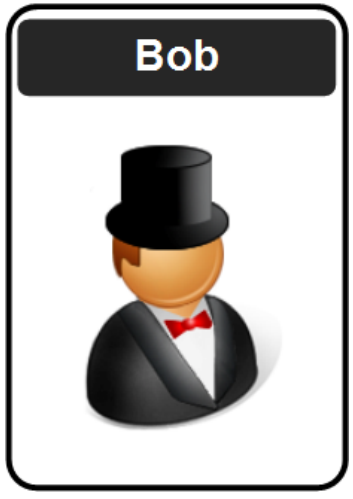
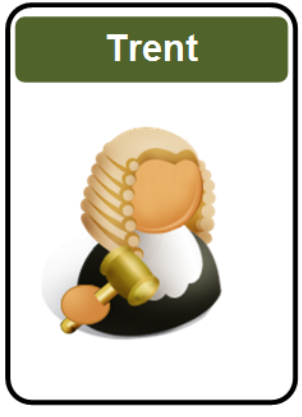
E-Security

1. Cryptography Fundamentals.
2. Symmetric Key Encryption.
3. Hashing and MAC.
4. Asymmetric (Public) Key Encryption.
5. Key Exchange.
6. Trust and Digital Certificates.
7. Tunnelling.
8. Cryptocurrencies and Blockchain.
9. Future Cryptography.
10. Host Security.

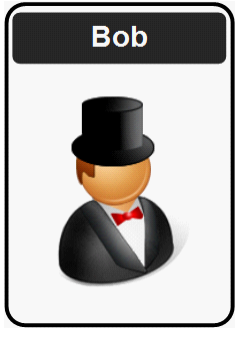
Prof Bill Buchanan OBE

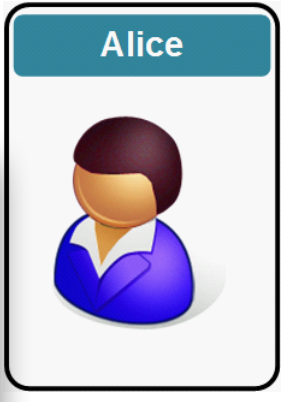
https://asecuritysite.com/encryption
https://asecuritysite.com/esecurity

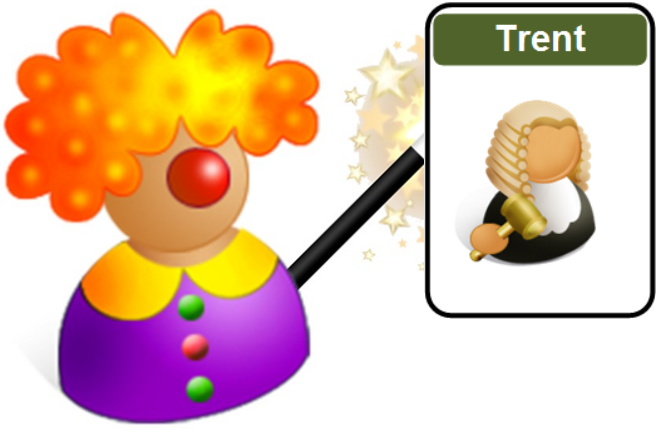




Disclaimer







- Encryption works great, until it doesn't.
- Encryption works great, as long as no one makes a mistake.
- Encryption works great, unless something goes wrong.
- Encryption works great, as long as everything works right.

Module Delivery

Web site

youtube.com

slack esecurityworkspace.com

Overleaf

@billatnapier

asecuritysite.com

github.com/billbuchanan/esecurity

Module Delivery

Web site

youtube.com

Lectures/Lab Demos

Overleaf

Coursework submission

ubuntu

Open SSL

Labs

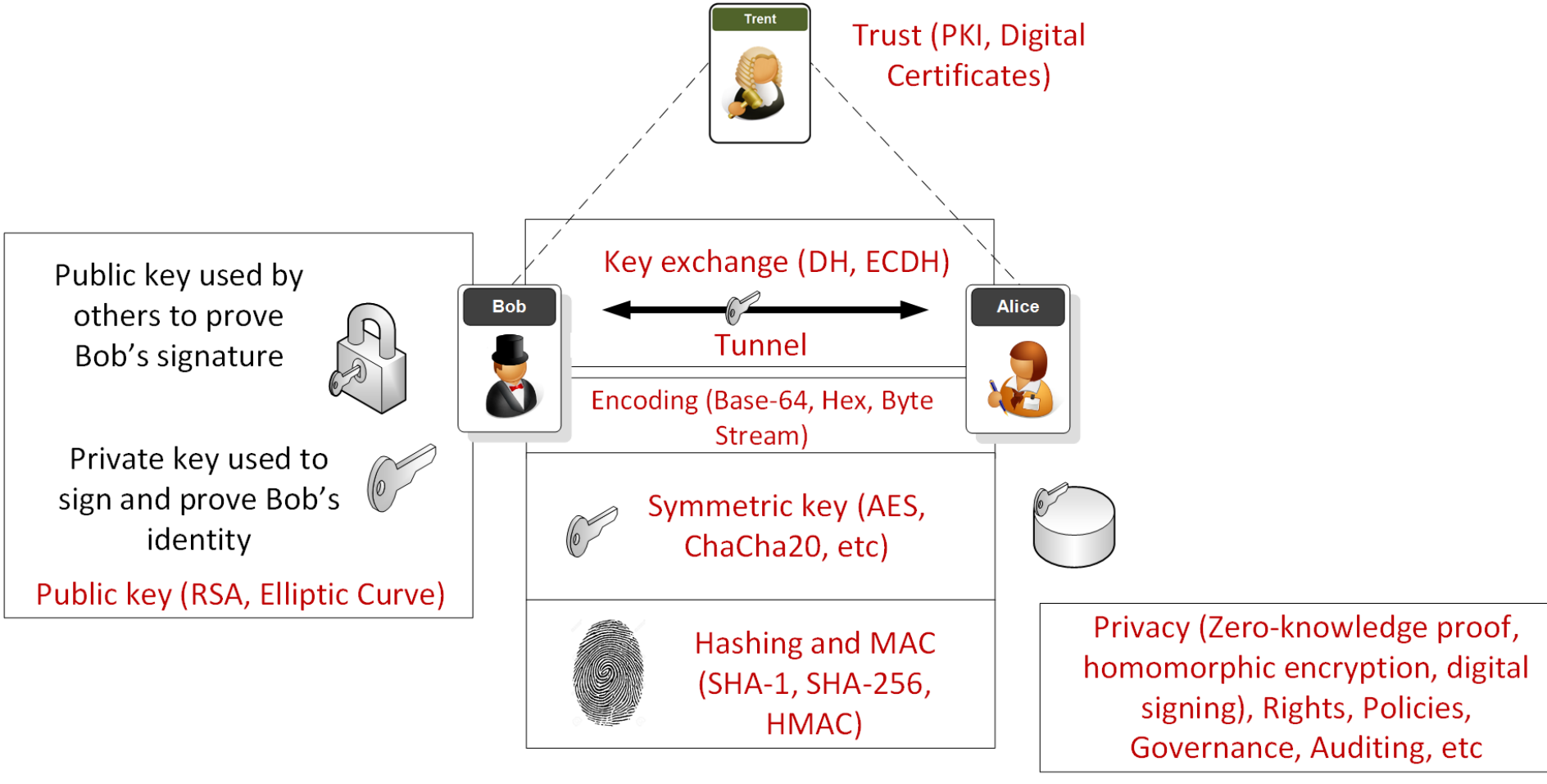
github.com/billbuchanan/esecurity

Draft Timetable

Web site

No	Date	Subject	Lab
1	18 Jan 2019	Ciphers and Fundamentals Unit	Lab [Link]
2	25 Jan 2019	Symmetric Key Unit	Lab [Link]
3	1 Feb 2019	Hashing and MAC Unit	Lab [Link]
4	8 Feb 2019	Asymmetric (Public) Key Unit	Lab [Link]
5	15 Feb 2019	Key Exchange Unit	Lab [Link]
6	22 Feb 2019	Guest lecture	Mini-project/Coursework
7	1 Mar 2019	Trust and Digital Certificates Unit	Lab [Link]
8	8 Mar 2019	Tunnelling Unit	Lab [Link]
9	15 Mar 2019	Test 1 (Units 1-7)	
10	22 Mar 2019	Blockchain Unit	Lab [Link]
11	29 Mar 2019	Future Cryptography Unit	Lab [Link]
12	5 April 2019	Host Security 1	
13	12 April 2019	Host Security 2	
Easter Break			
14	29 April 2019	Test 2 (Units 8-12)	
15	6 May 2019	Coursework Hand-in	

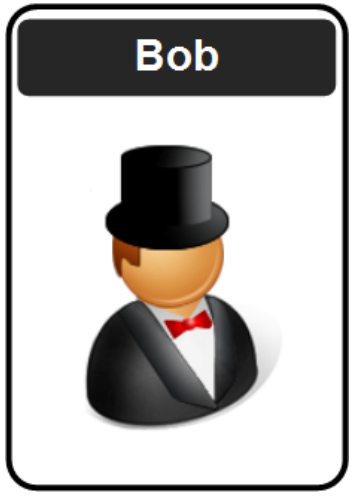
Overview

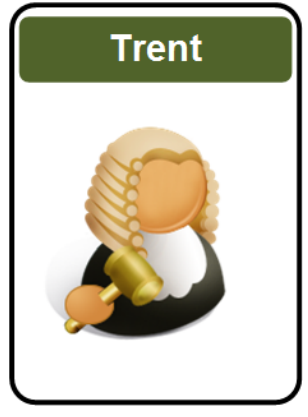

Trent
Trust (PKI, Digital Certificates)
Public key used by others to prove Bob's signature
Private key used to sign and prove Bob's identity
Public key (RSA, Elliptic Curve)
Bob
Key exchange (DH, ECDH)
Tunnel
Alice
Encoding (Base-64, Hex, Byte Stream)
Symmetric key (AES, ChaCha20, etc)
Hashing and MAC (SHA-1, SHA-256, HMAC)
Privacy (Zero-knowledge proof, homomorphic encryption, digital signing), Rights, Policies, Governance, Auditing, etc

1. Fundamentals

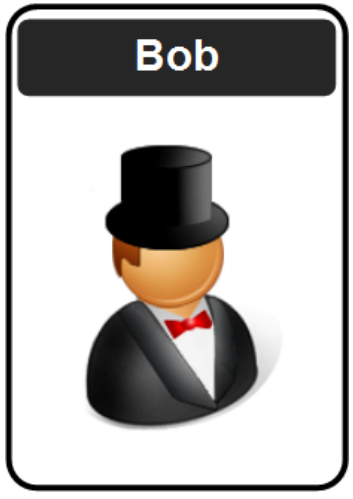
Traditional Ciphers.
Key-based Encryption.
Encoding Methods.
Frequency Analysis.
GCD.
Random Numbers.
Prime Numbers.
Big Integers.
Encryption Operators (MOD, XOR and Shift).

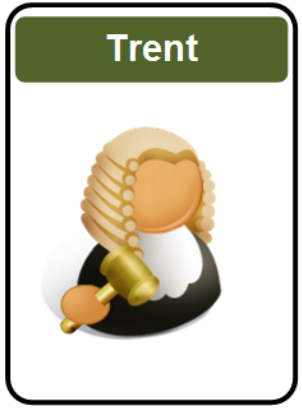
Prof Bill Buchanan OBE
https://asecuritysite.com/encryption





2. Symmetric Key

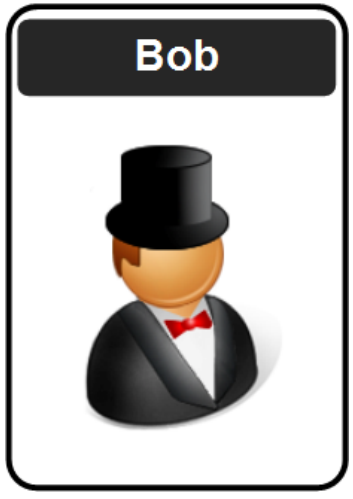




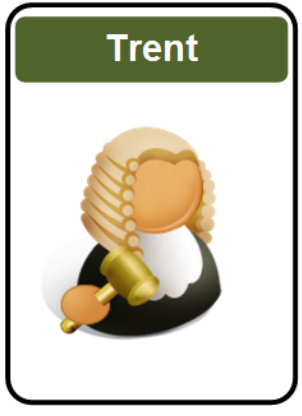
Basics
Block or Stream?
Secret Key Methods
Salting
AES
3DES
ChaCha20/Poly1305
Key Entropy

Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

3. Hashing and MAC



Hashing Methods.
Cracking.
Typical Methods: MD5, SHA-1, SHA-3, LM, Bcrypt, PBKDF2
Hashed Passwords.
Timed One Time Passwords.
Message Authentication Codes (MACs).

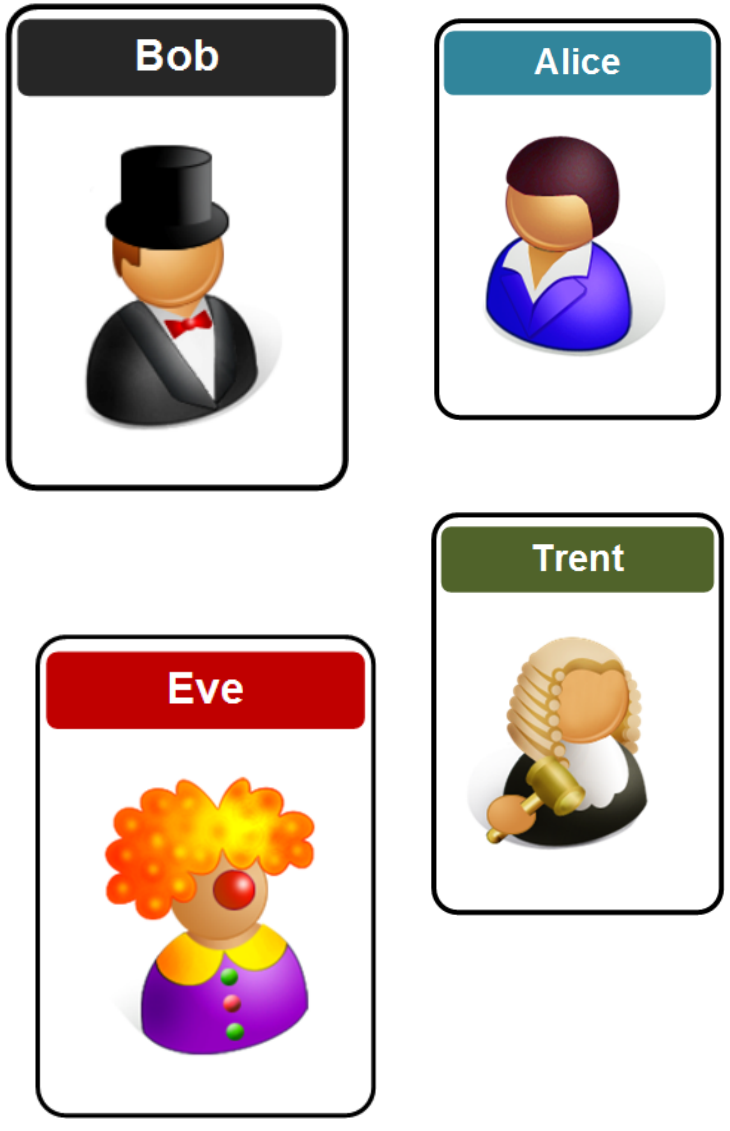


Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

4. Asymmetric Key

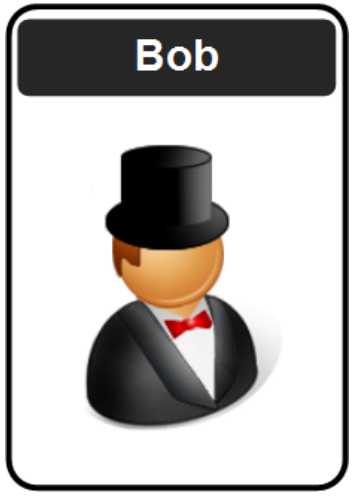
Principles.
RSA.
Elliptic Curve.
Using Private Key to Authenticate.
PGP: Signed Email.

Prof Bill Buchanan OBE
https://asecuritysite.com/encryption



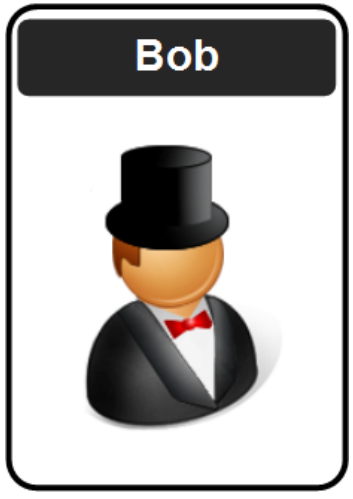
5. Key Exchange

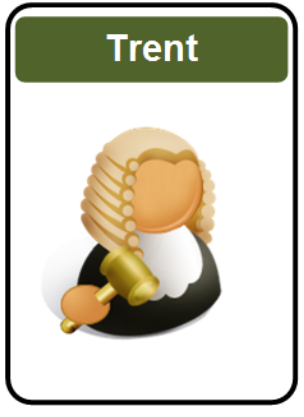
Principles.
Diffie-Hellman (DH).
Passing the secret key with key exchange.
Elliptic Curve Diffie-Hellman (ECDH)



Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

6. Trust and Digital Certificates





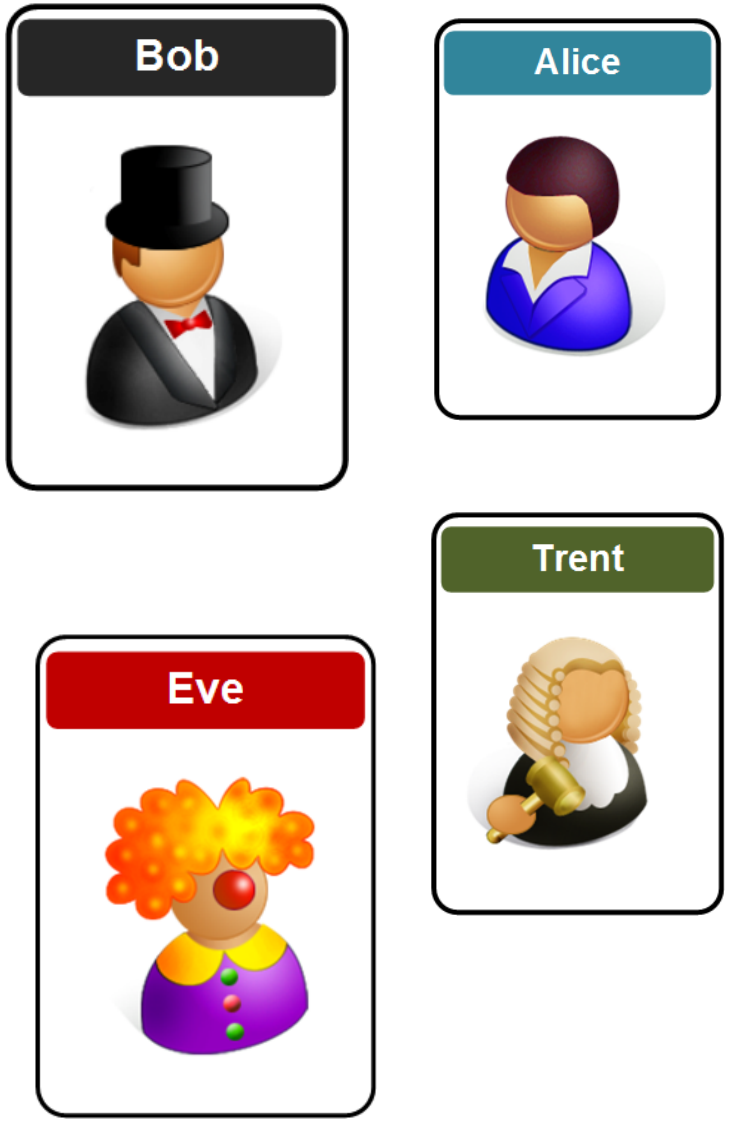
Principles.
Trust Infrastructures.
PKI Infrastructure.
Creating Signed Certificates.
Signatures (ECDSA, Hashed-based).

Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

7. Tunnelling

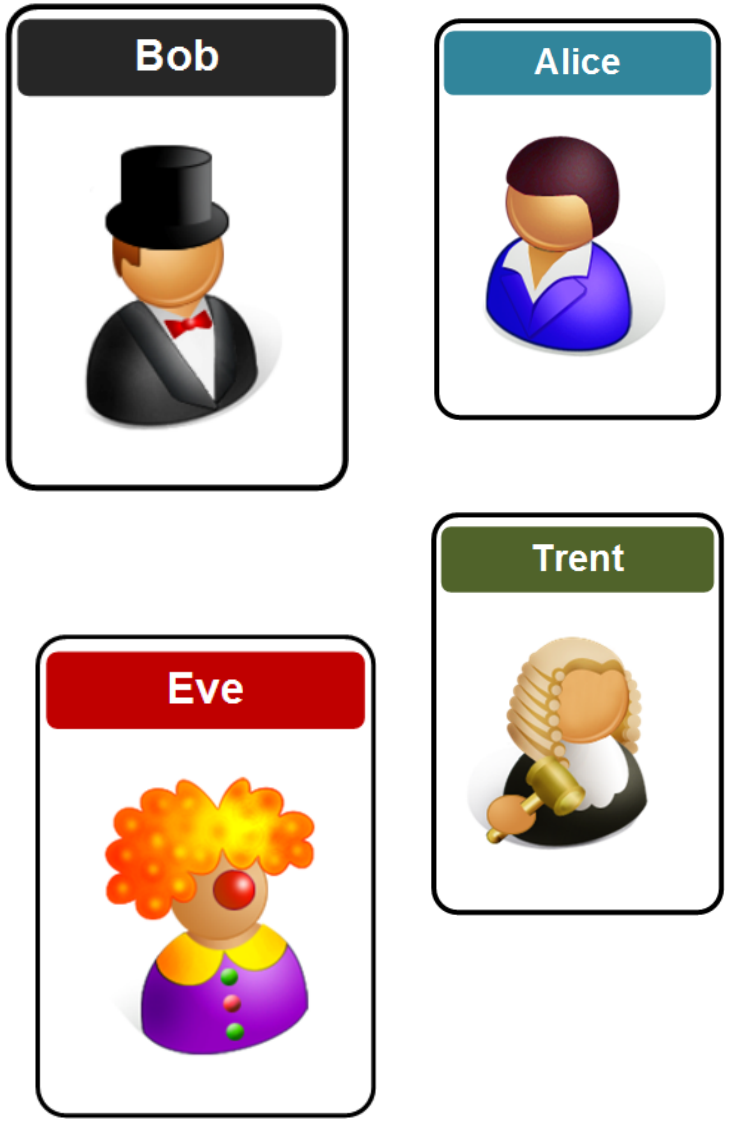
SSL/TLS.
Key generation/key exchange.
SSH.
IPSec.

Prof Bill Buchanan OBE
https://asecuritysite.com/encryption



8. Blockchain & Cryptocurrencies

Principles.
Bitcoin.
Ethereum.
Smart Contracts.



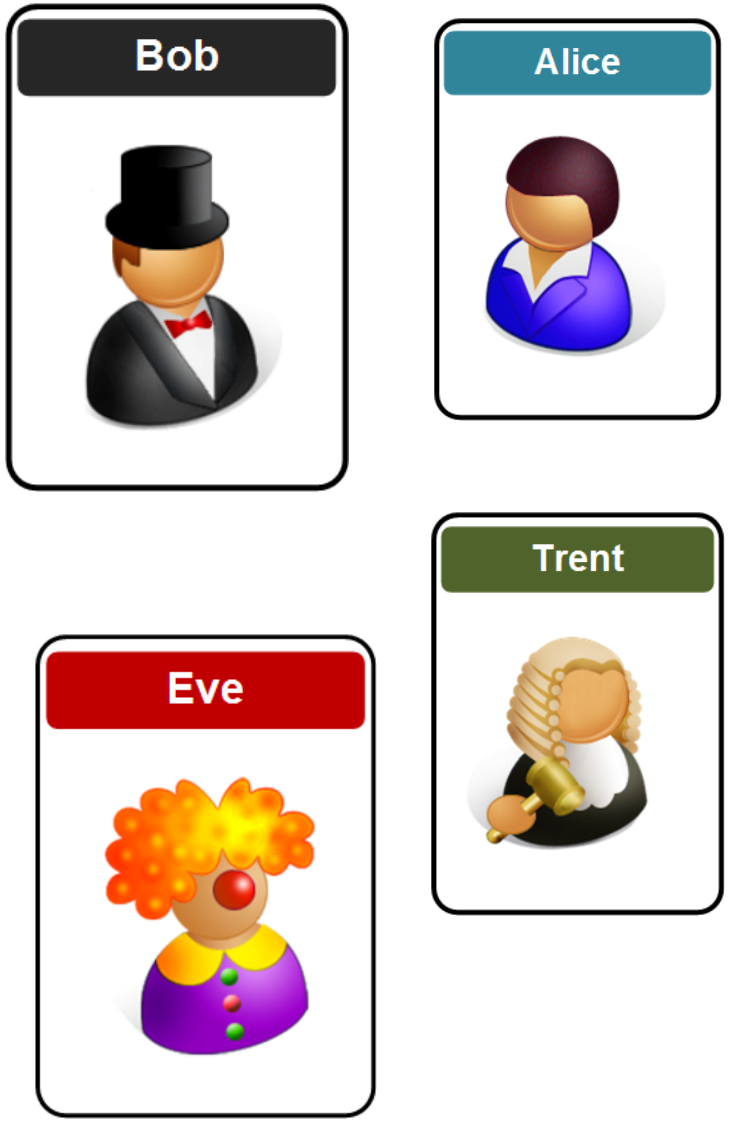
Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

9. Future Crypto

Zero knowledge proof.
Homomorphic encryption.
Light-weight crypto.
Quantum-robust cryptography.

Prof Bill Buchanan OBE

https://asecuritysite.com/encryption



E-Security

1. Cryptography Fundamentals.
2. Symmetric Key Encryption.
3. Hashing and MAC.
4. Asymmetric (Public) Key Encryption.
5. Key Exchange.
6. Trust and Digital Certificates.
7. Tunnelling.
8. Cryptocurrencies and Blockchain.
9. Future Cryptography.
10. Host Security.

Prof Bill Buchanan OBE

https://asecuritysite.com/encryption
https://asecuritysite.com/esecurity