Apl

1. Cryp
2. Symr
3. Hash
4. Asyn
5. Key E
6. Trust
7. Tunn
8. Cryp
9. Futu
10. Hos

Prof

https:/
https:/

Citizen rights to access their own data

Detect
Respond
Investigate

Incident Response

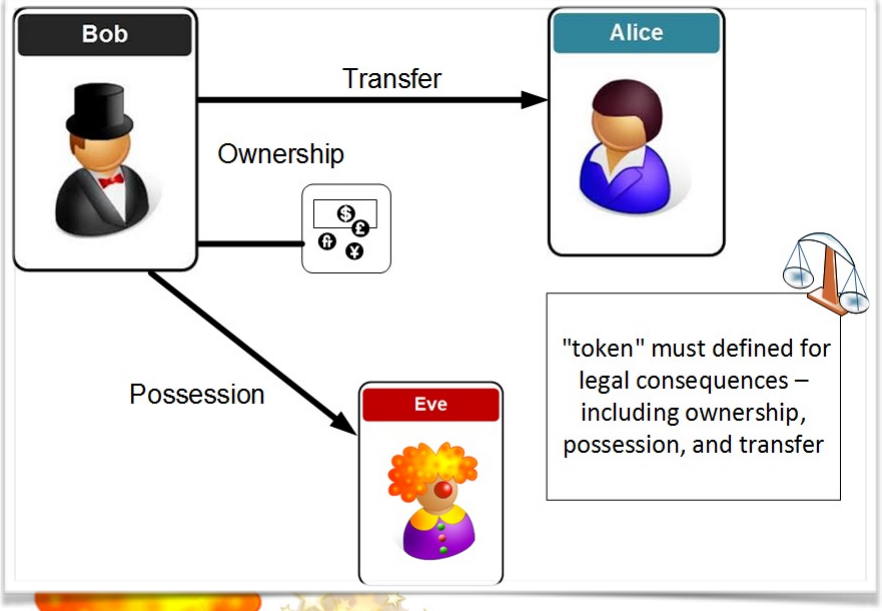
Encryption

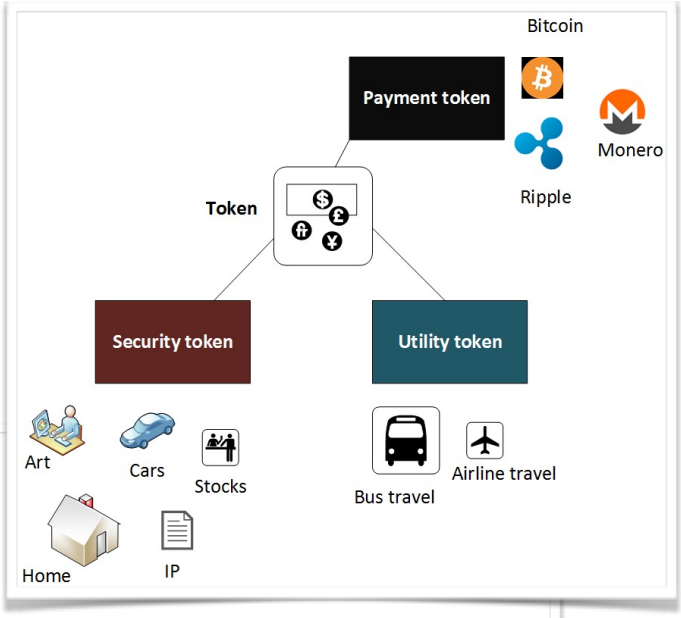
Pseudo-anonymity

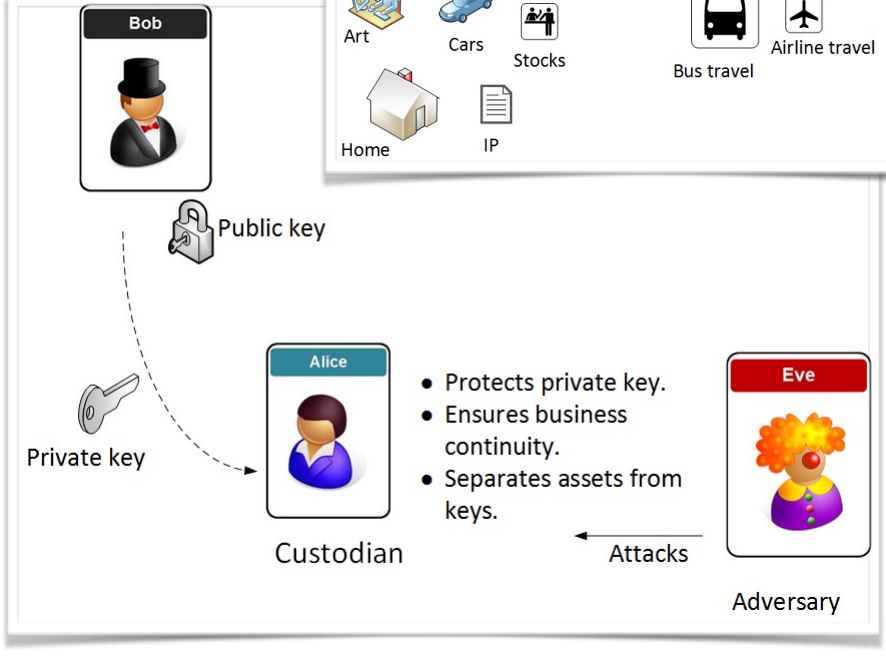
Alice

Trent

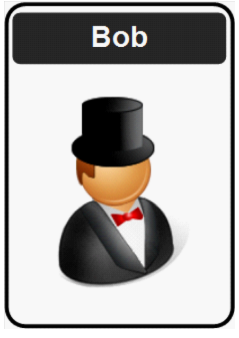
A Tokenized World …

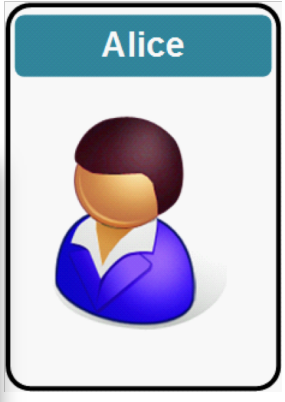


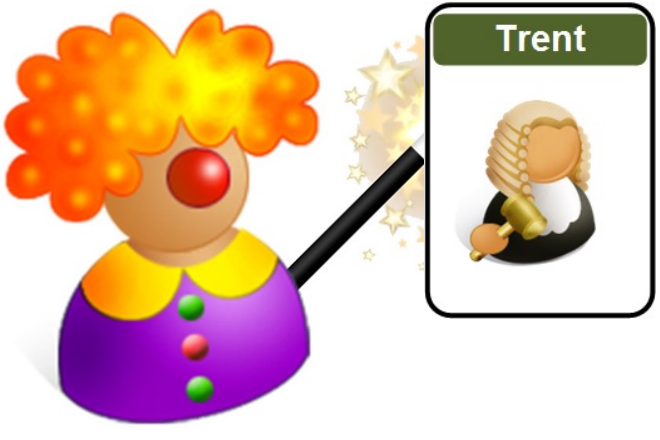




Disclaimer







- 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

Teams

Overleaf

@billatnapier

asecuritysite.com

github.com/billbuchanan/appliedcrypto

Module Delivery

Web site

youtube.com

Lectures/Lab Demos

Overleaf

Coursework submission

ubuntu

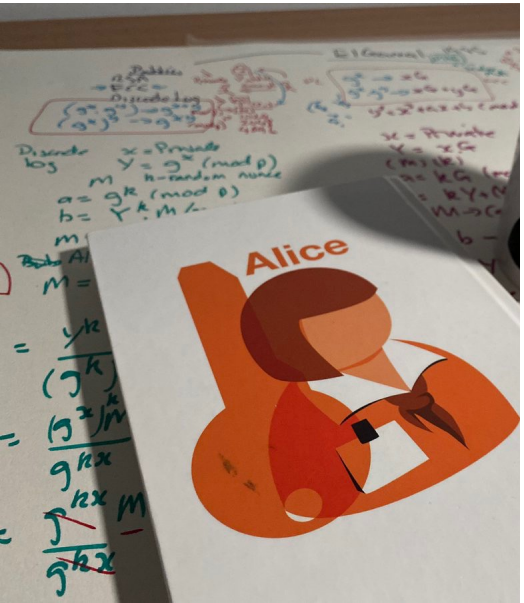
Open SSL

node JS

Labs github.com/billbuchanan/appliedcrypto

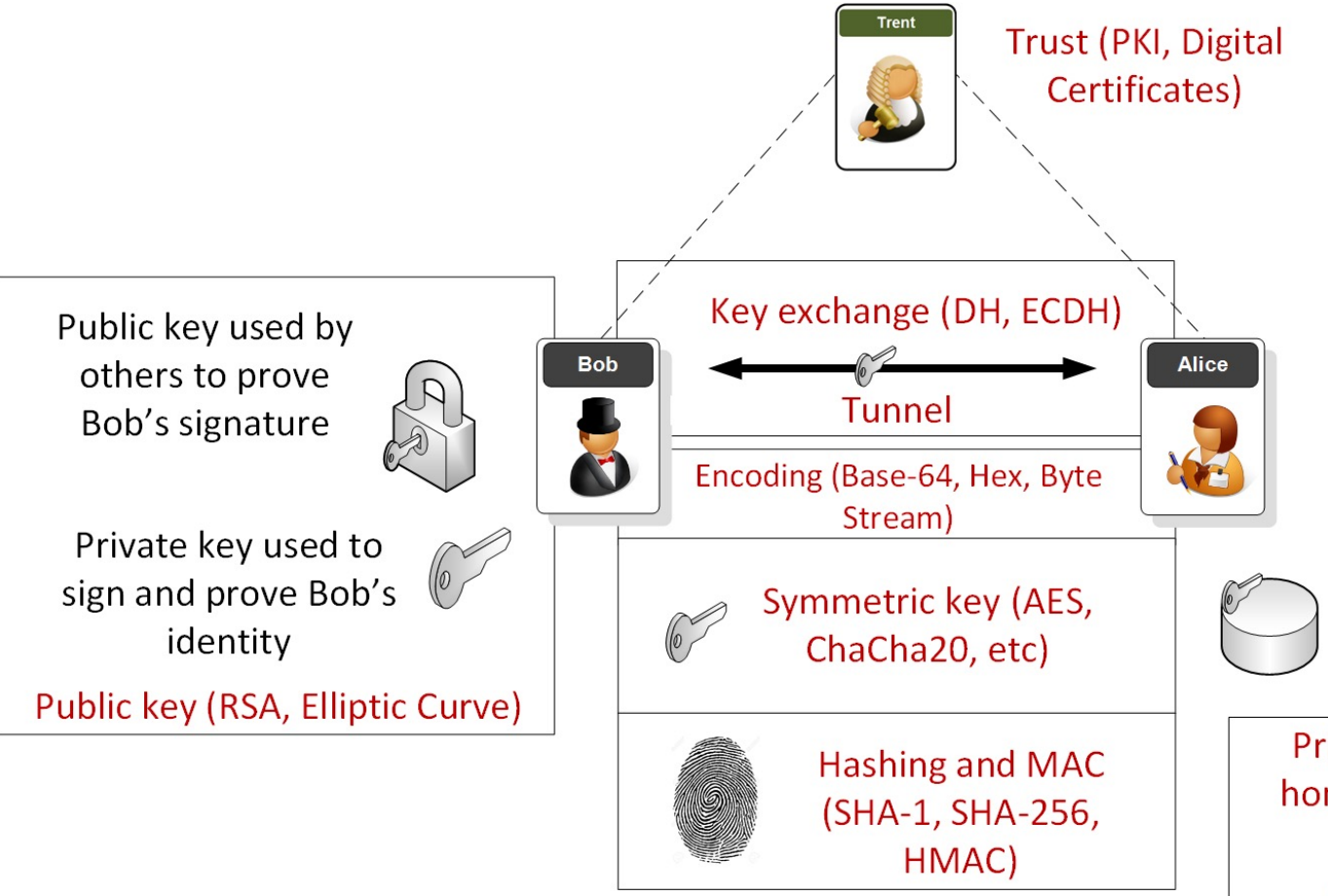
Draft Timetable

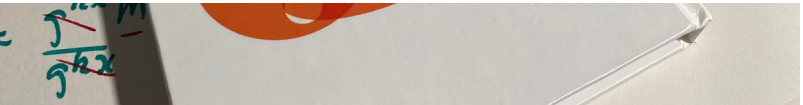
Web site



No	Date	Subject	Lab
2	28 Jan 2021	Ciphers and Fundamentals Unit	Lab Demo
3	4 Feb 2021	Symmetric Key	Lab
4	11 Feb 2021	Hashing and MAC	Lab
5	18 Feb 2021	Asymmetric (Public) Key	Lab
6	25 Feb 2021	Key Exchange	Lab
7	4 Mar 2021	Digital Signatures and Certificates	Lab
8	11 Mar 2021	Revision lecture and Test 1/Coursework	Mini-project/Coursework
9	18 Mar 2021	Test (Units 1-5) 40% of overall mark	
10	25 Mar 2021	Tunnelling	Lab
11	1 Apr 2021		Guest talk
12	8 Apr 2021	Blockchain	Lab
13	29 Apr 2021	Future Cryptography	Lab
14	6 May 2021		Lab
15	13 May 2021	Coursework Hand-in - 60% of overall mark	

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
Alice
Key exchange (DH, ECDH)
Tunnel
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

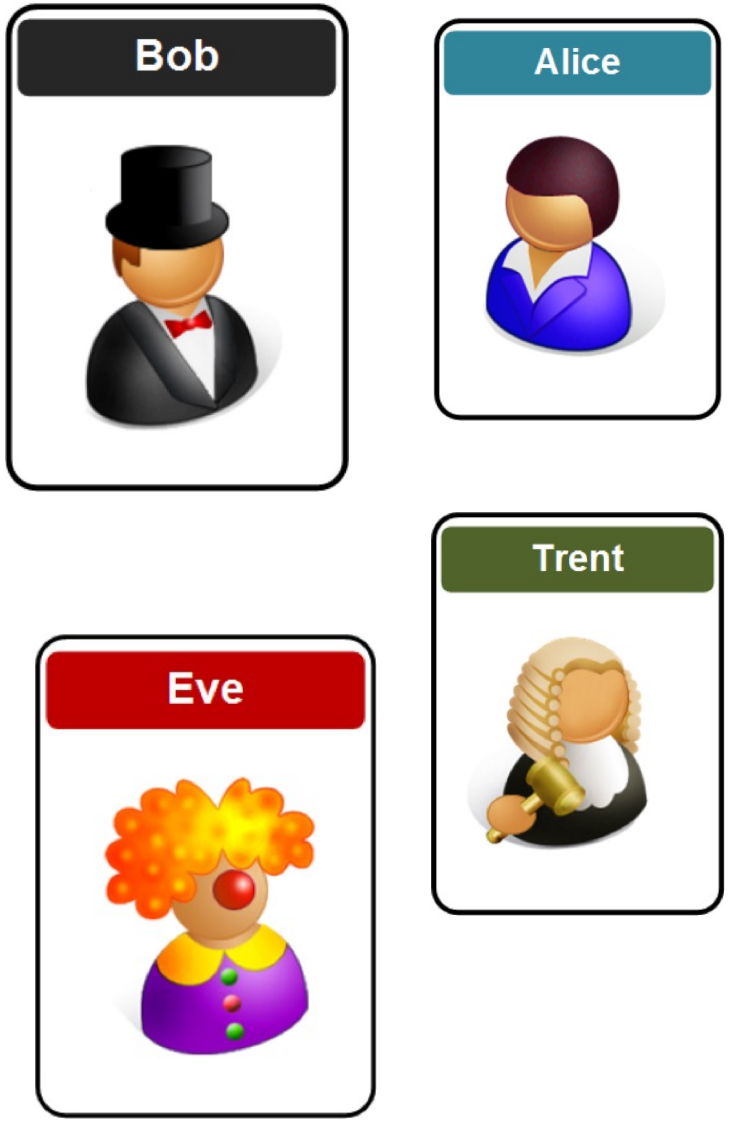
Traditional Ciphers.
Key-based Encryption.
Encoding Methods.
Frequency Analysis.
GCD.
Random Numbers.
Prime Numbers.
Big Integers.
Encryption Operators (MOD, XOR and Shift).

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

2. Symmetric Key

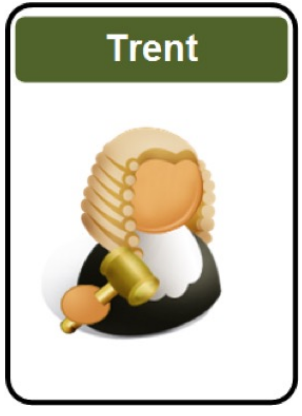
Basics
Block or Stream?
Secret Key Methods
Salting
AES
3DES
ChaCha20/Poly1305
Key Entropy

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



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).

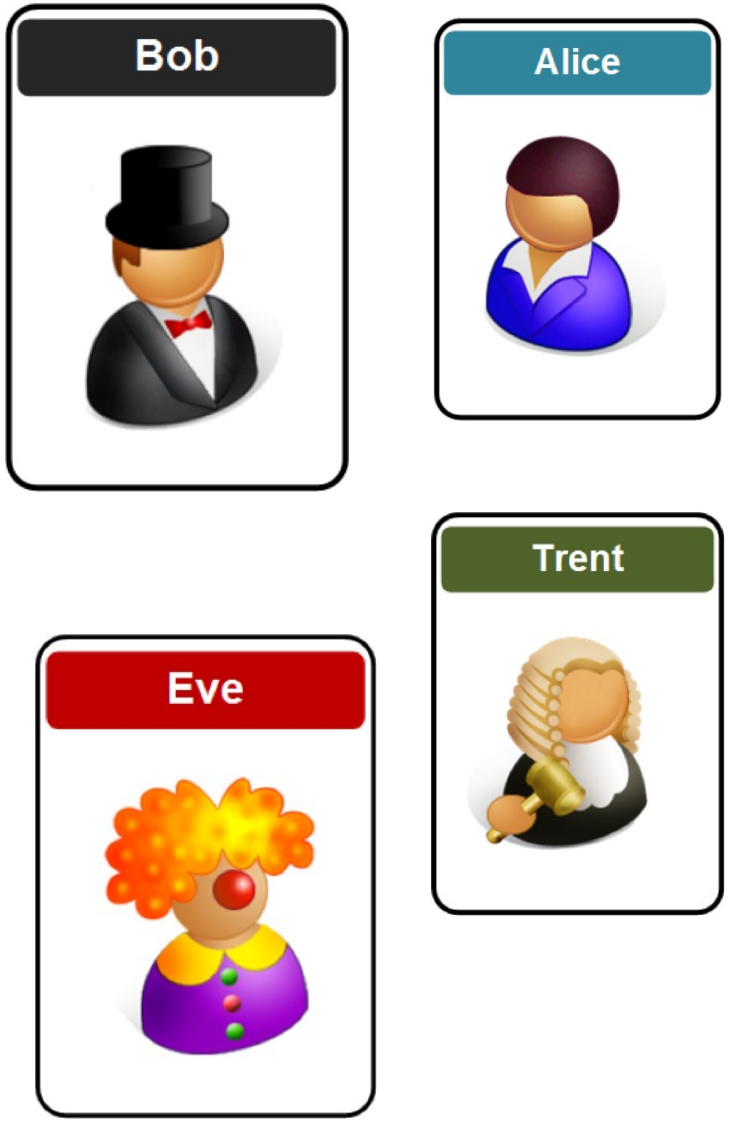


Prof Bill Buchanan OBE
https://asecuritysite.com/

4. Asymmetric Key

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

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



5. Key Exchange

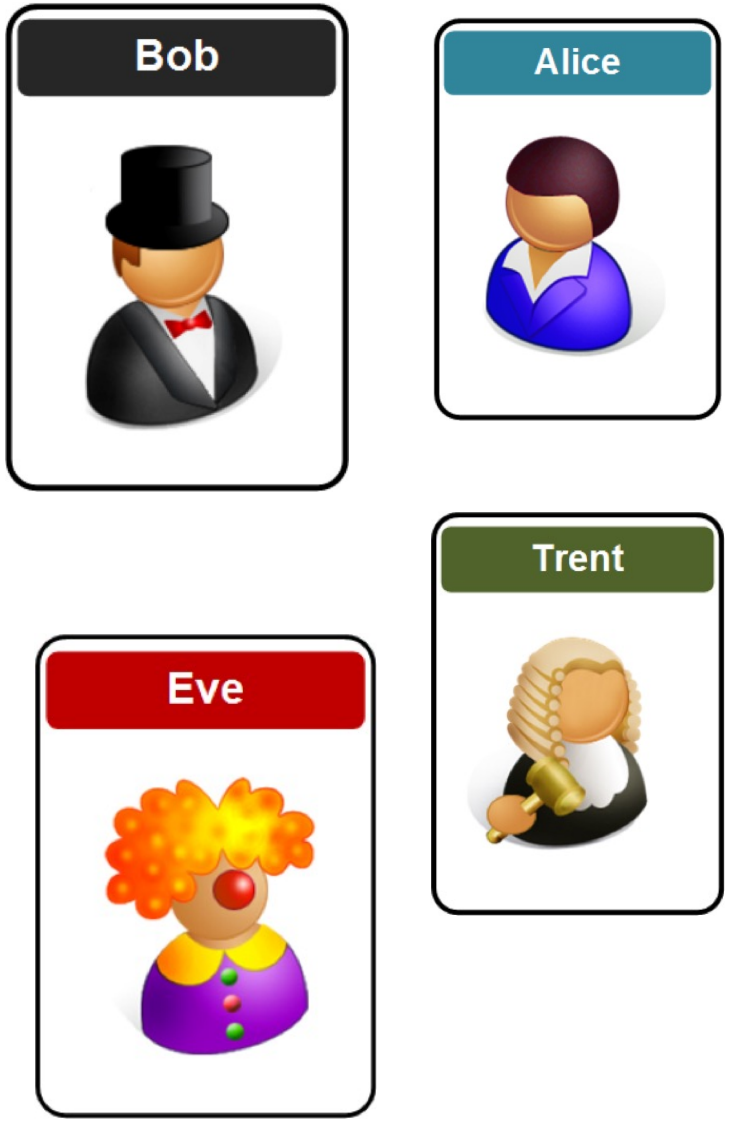
Principles.
Diffie-Hellman (DH).
Passing the secret key with key exchange.
Elliptic Curve Diffie-Hellman (ECDH)

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

6. Signatures and Digital Certificates

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

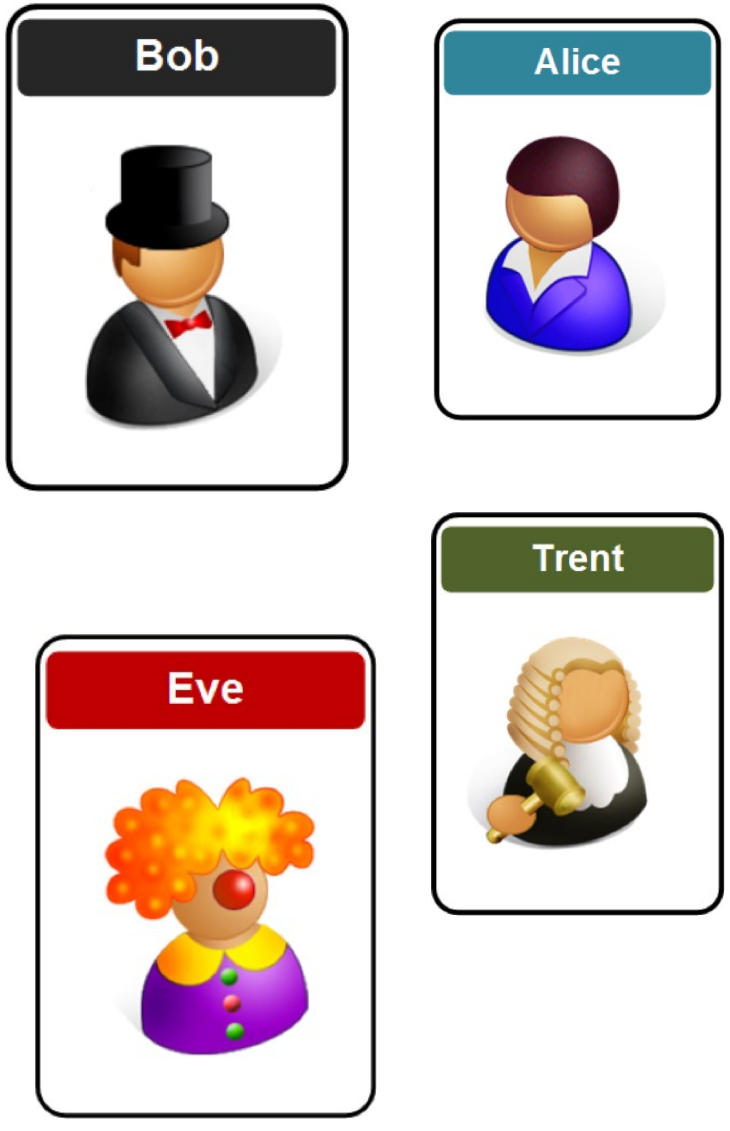
Prof Bill Buchanan OBE
https://asecuritysite.com/



7. Tunnelling

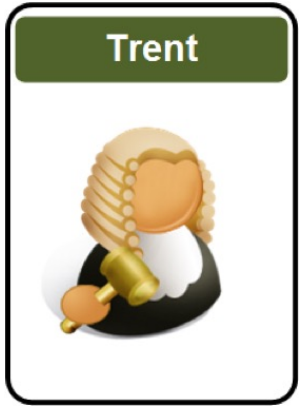
SSL/TLS.
Key generation/key exchange.
SSH.
IPSec.

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



8. Blockchain & Cryptocurrencies

Principles.
Bitcoin.
Ethereum.
Smart Contracts.

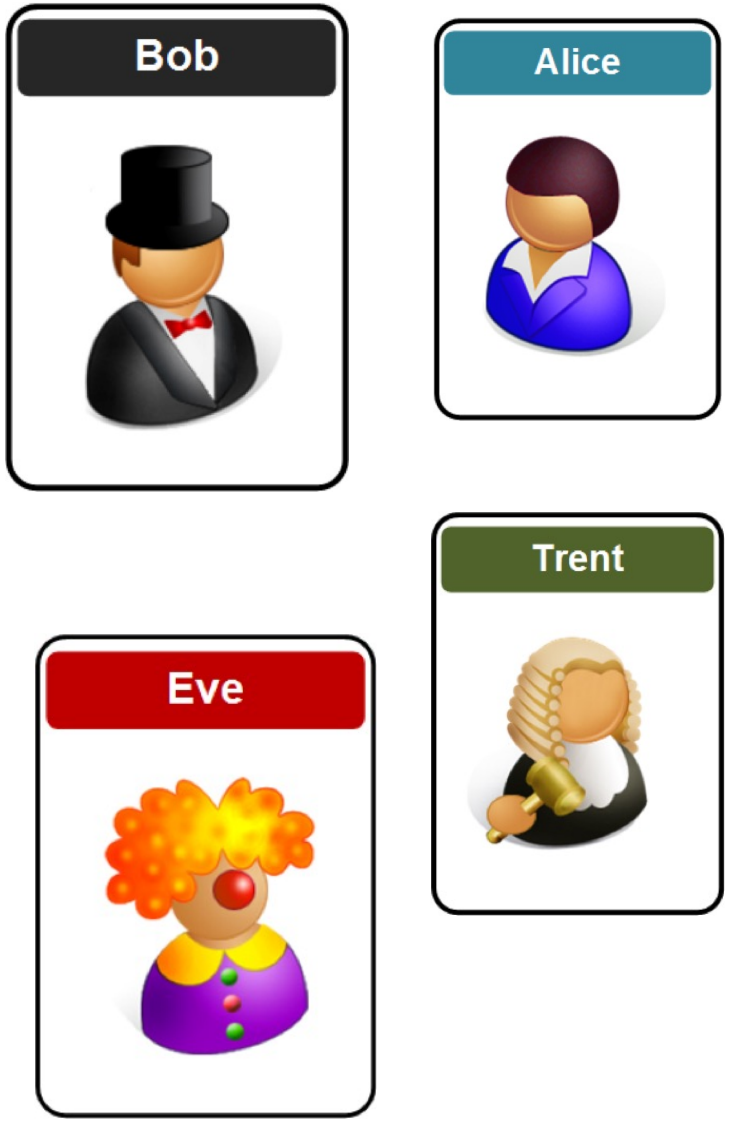


Prof Bill Buchanan OBE
https://asecuritysite.com/

9. Future Crypto

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

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



Applied Cryptography

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

Prof Bill Buchanan OBE

https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto