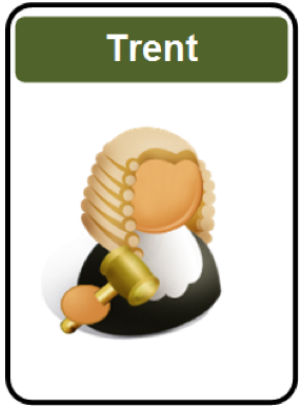
Applied Crypto: Introduction

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/Cloud Security.

Prof Bill Buchanan OBE

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



A

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Pr

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

Citizen rights to access their own data

Detect
Respond
Investigate

Incident Response

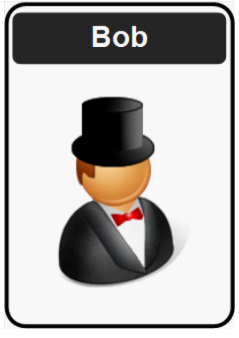
Encryption

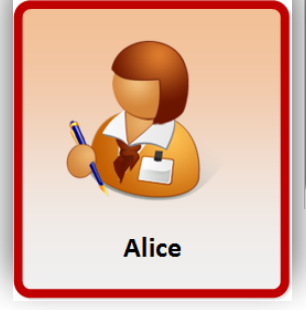
Pseudo-anonymity

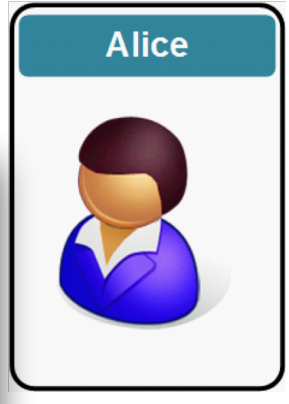
Alice

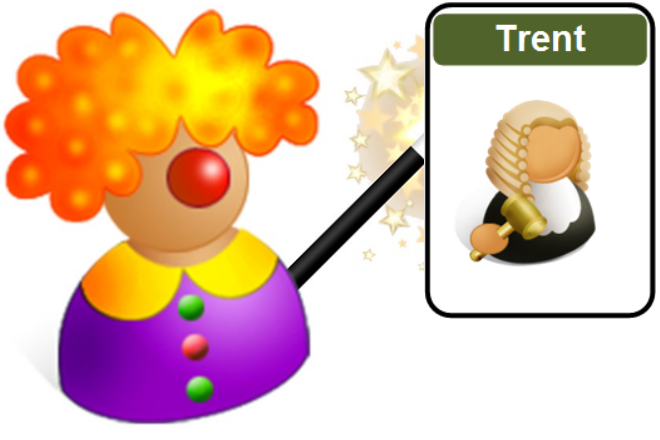
Trent

Disclaimer



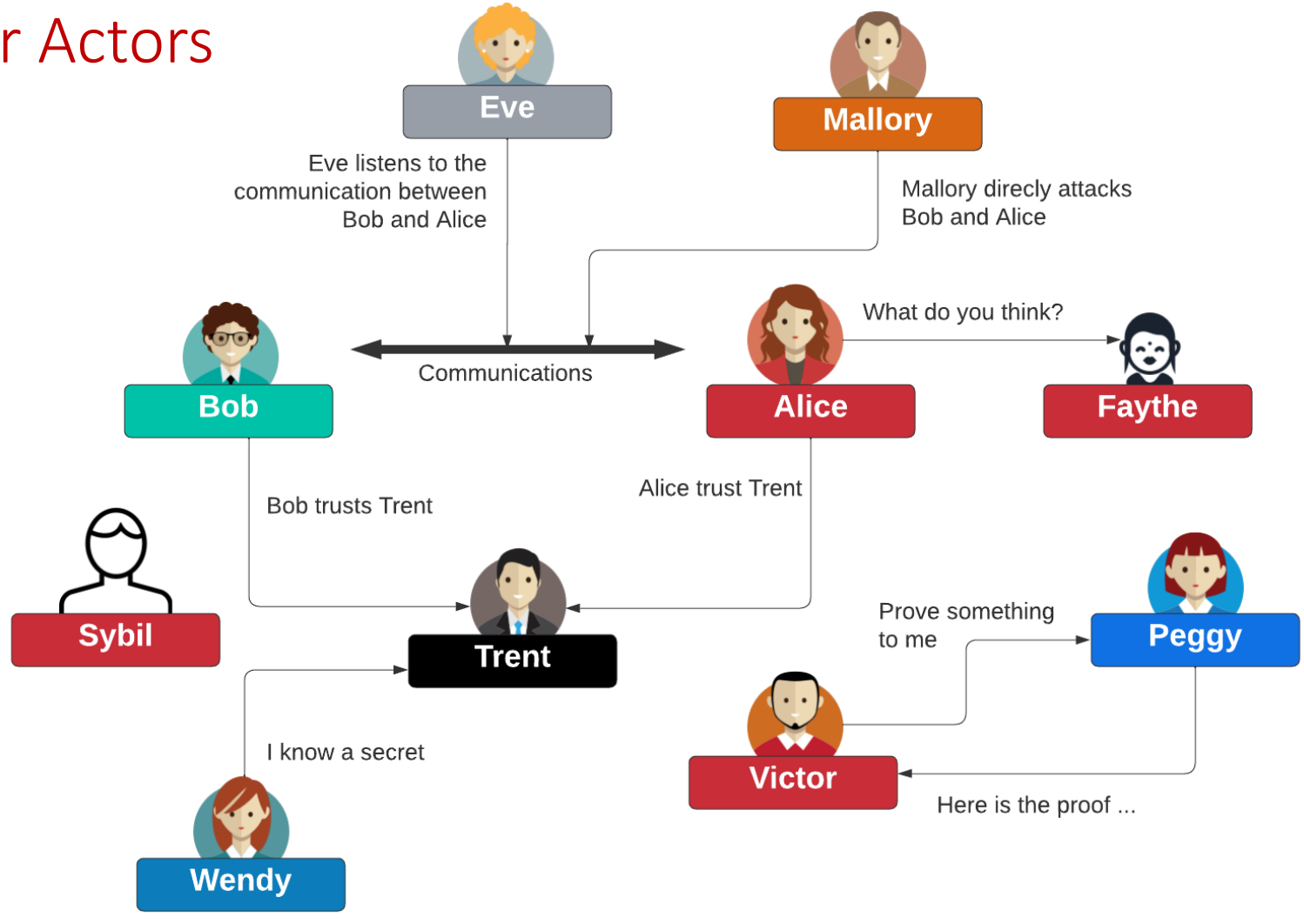






- Encryption works great, until it doesn't.
- Encryption works great, as long as no one makes a mistake.
- Encryption works great, unless something goes wrong.
- Encryption works great, as long as everything works right.

Cyber Actors



Module Delivery

Web site

youtube.com

Teams

Overleaf

@billatnapier

asecuritysite.com

github.com/billbuchanan/appliedcrypto

Module Delivery

Web site

youtube.com

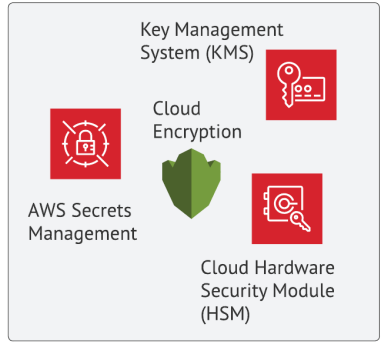
Lectures/Lab Demos

Overleaf

Coursework submission

ubuntu

OpenSSL



Labs github.com/billbuchanan/appliedcrypto

Draft Timetable

Web site

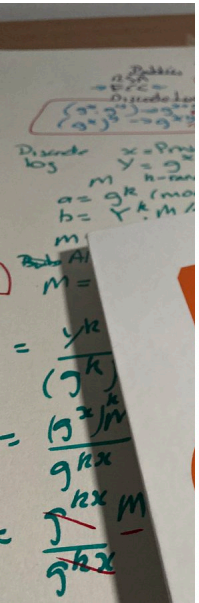
CSN11131 (Applied Cryptography and Trust)

9-11am Lecture (A.17 or Teams)	Principles Demos Menti Test
11-1pm Lab (C.27 or Teams)	vSoC 2 or AWS
6-7pm Evening Session (Teams)	Recap Menti Test (Guest Talk)

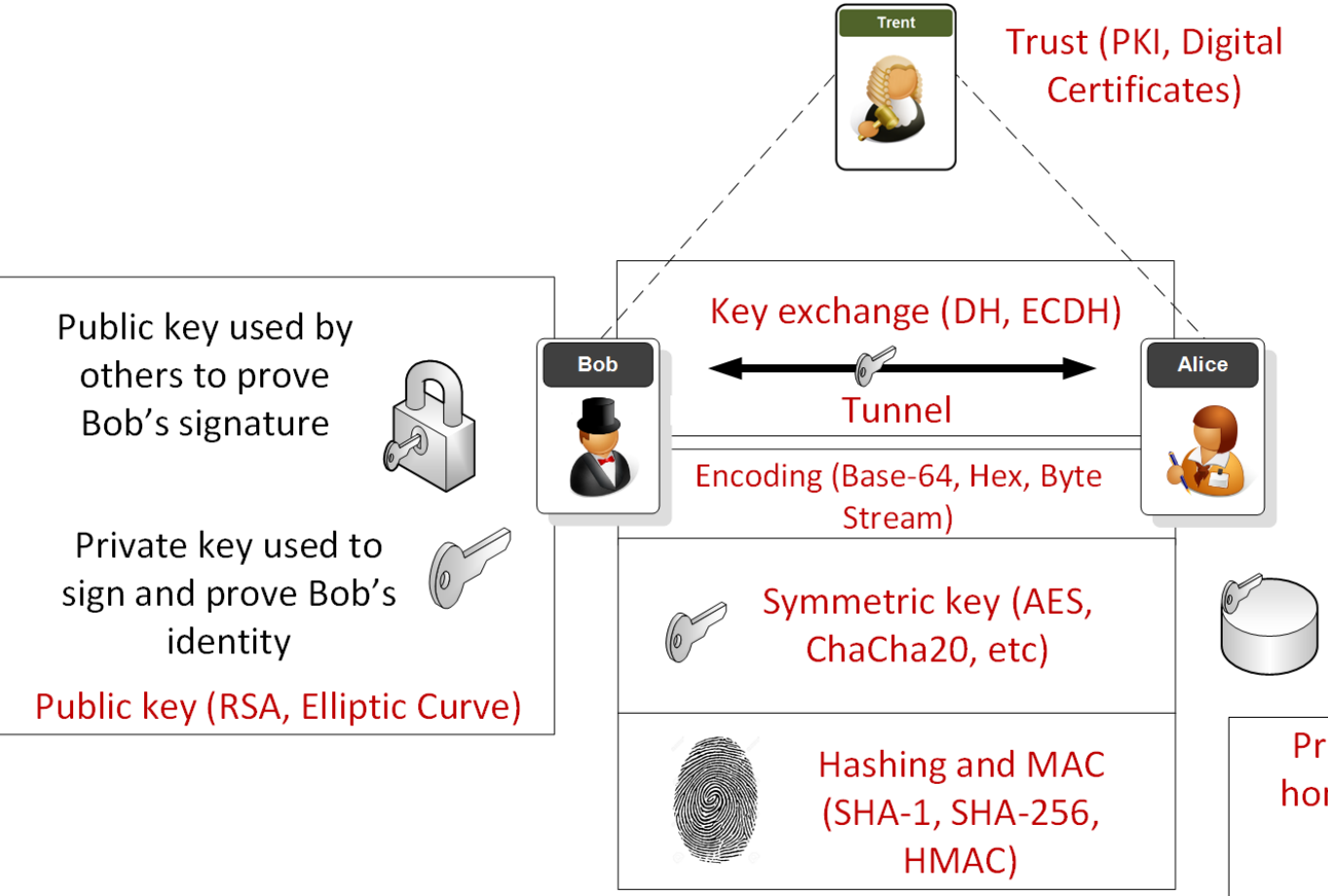
Draft Timetable

Web site

No	Date	Subject	Lab
2	27 Jan 2023	Ciphers and Fundamentals [Unit]	[Lab] [Demo]
3	3 Feb 2023	Symmetric Key [Unit]	[Lab]
4	10 Feb 2023	Hashing and MAC [Unit]	[Lab]
5	17 Feb 2023	Asymmetric (Public) Key [Unit]	[Lab]
6	24 Feb 2023	Key Exchange [Unit]	[Lab]
7	3 Mar 2022	Digital Signatures and Certificates [Unit]	[Lab]
8	11 Mar 2023	Revision lecture and Test 1/Coursework	Mini-project [Here] /Coursework
9	17 Mar 2023	Test (Units 1-5) 40% of overall mark [Here]	
10	24 Mar 2023	Tunnelling [Unit]	[Lab]
11	31 Mar 2023	Blockchain [Unit]	[Lab]
12	28 Apr 2023	Future Cryptography [Unit]	[Lab]
13	5 May 2023	Host/Cloud Security [Unit]	[Lab]
14	12 May 2023		
15	19 May 2023	Coursework Hand-in - 60% of overall mark (15 May)	



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)
Alice
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/
https://github.com/billbuchanan/appliedcrypto

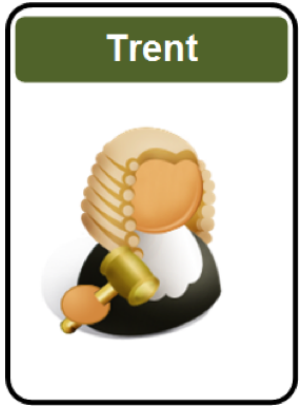
2. Symmetric Key

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

Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto

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

4. Asymmetric Key

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

Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto

5. Key Exchange

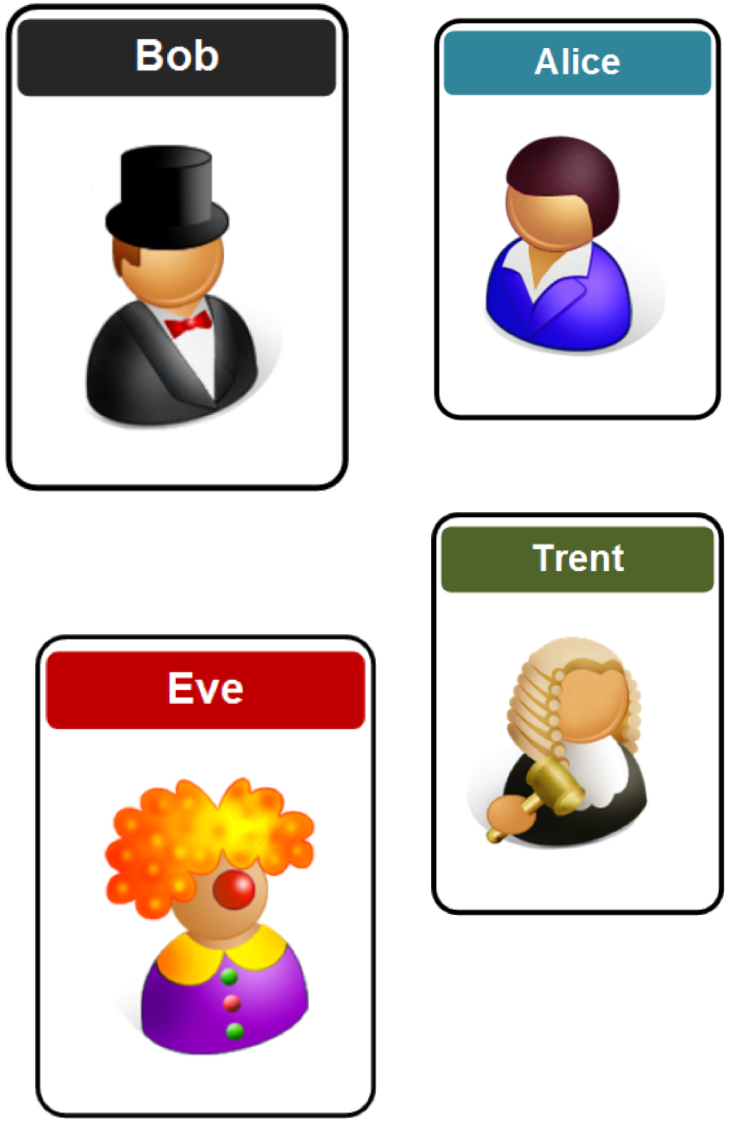
Principles.
Diffie-Hellman (DH).
Passing the secret key with key exchange.
Elliptic Curve Diffie-Hellman (ECDH)

Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto

6. Signatures and Digital Certificates

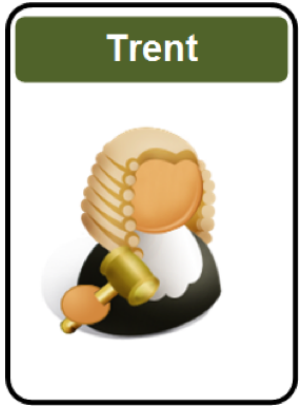
Principles.
Trust Infrastructures.
PKI Infrastructure.
Creating Signed Certificates.
Signatures (DSA, ECDSA, Hashed-based).

Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto



7. Tunnelling

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



Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto

8. Blockchain & Cryptocurrencies

Principles.
Bitcoin.
Ethereum.
Smart Contracts.

Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto

9. Future Crypto

Zero knowledge proof.
Homomorphic encryption.
Light-weight cryptography.
Quantum-robust cryptography.
Secure Enclaves/Host Trust.

Prof Bill Buchanan OBE
https://asecuritysite.com/
https://github.com/billbuchanan/appliedcrypto

10. Host/Cloud

Trust Infrastructures.
Secure Enclaves.
Hardware/Software Tokens. FIDO2.
Biometric cryptography.

Prof Bill Buchanan OBE

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

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.
10. Host/Cloud Security.

Prof Bill Buchanan OBE

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