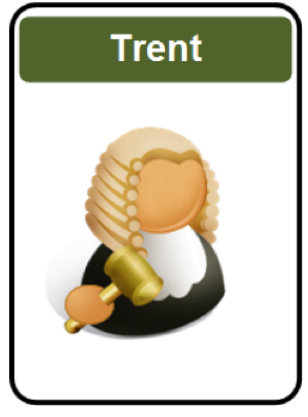
Applied Crypto: Introduction

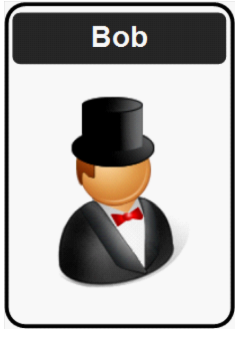
1. Cryptography Fundamentals.
2. Symmetric Key Encryption.
3. Hashing and MAC.
4. Asymmetric (Public) Key Encryption.
5. Key Exchange.
6. Trust and Digital Certificates.
7. Tunnelling.
8. Cryptocurrencies and Blockchain.
9. Future Cryptography.
10. Host/Cloud Security.

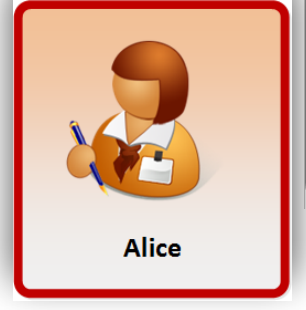
Prof Bill Buchanan OBE FRSE

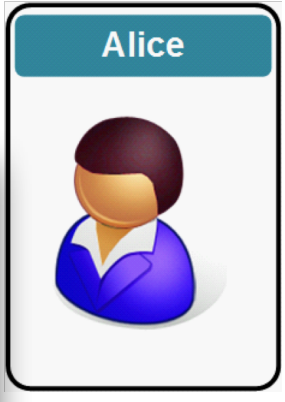
https://asecuritysite.com
https://github.com/billbuchanan/appliedcrypto

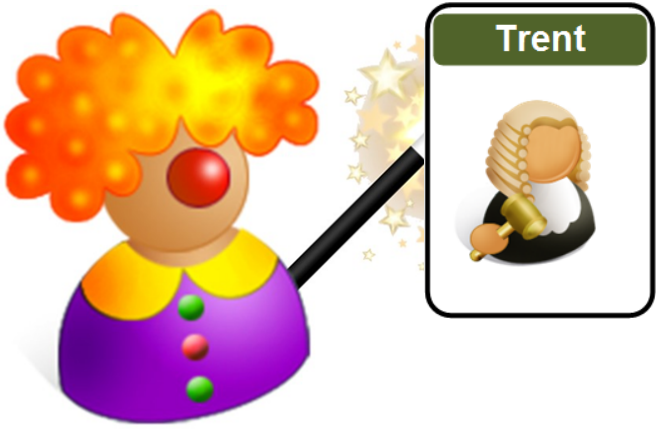


Disclaimer



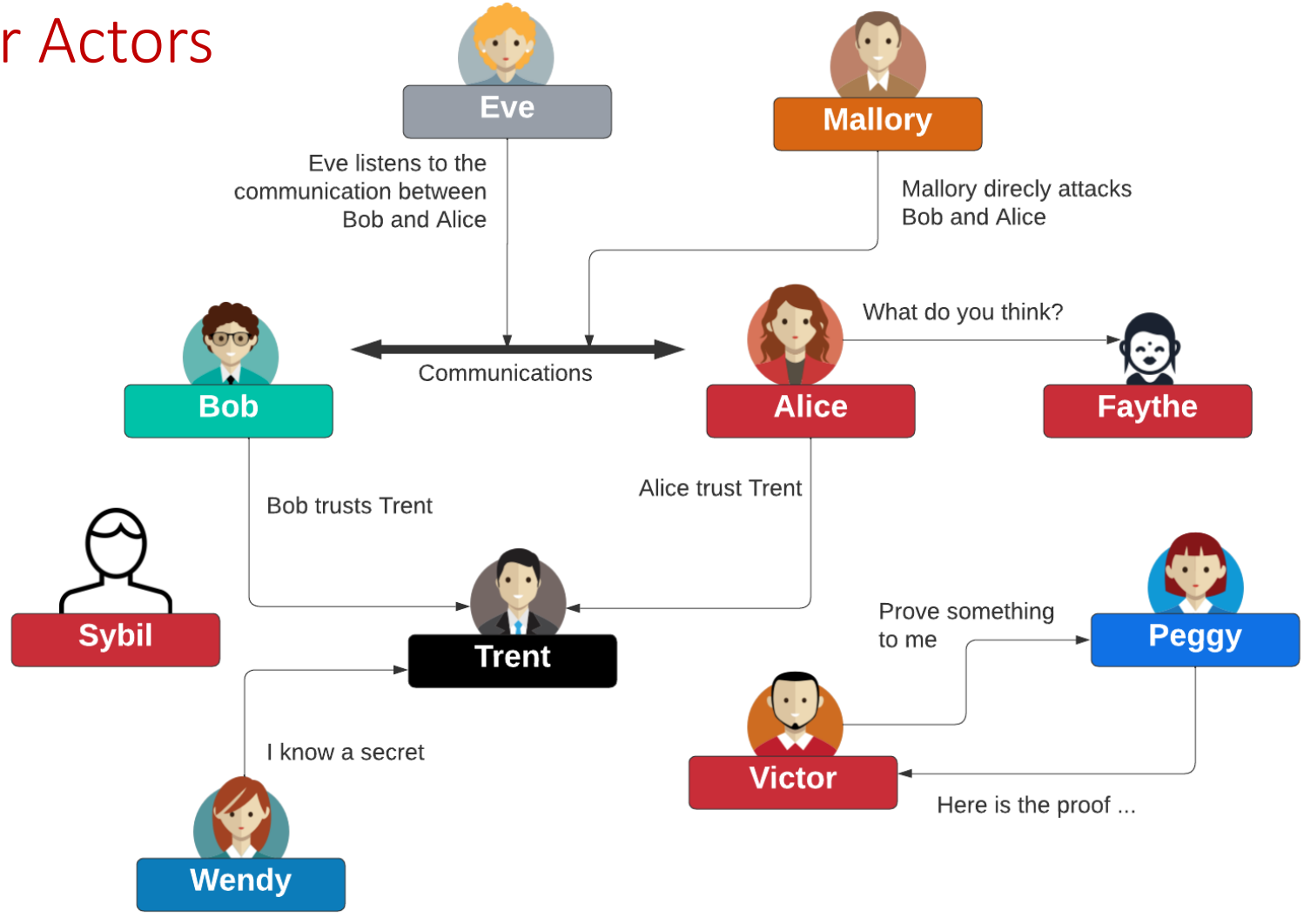






- Encryption works great, until it doesn't.
- Encryption works great, as long as no one makes a mistake.
- Encryption works great, unless something goes wrong.
- Encryption works great, as long as everything works right.

Cyber Actors



Module Delivery

Web site

youtube.com

Teams

Overleaf

@billatnapier

asecuritysite.com

github.com/billbuchanan/appliedcrypto

Module Delivery

Web site

youtube.com

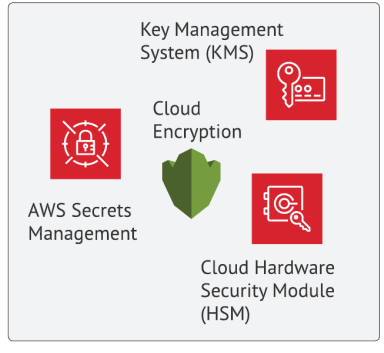
Lectures/Lab Demos

Overleaf

Coursework submission

ubuntu

OpenSSL



Labs github.com/billbuchanan/appliedcrypto

Draft Timetable

Web site

9-11am: Lecture (G24 or Teams – Principles, Demos and Menti Test

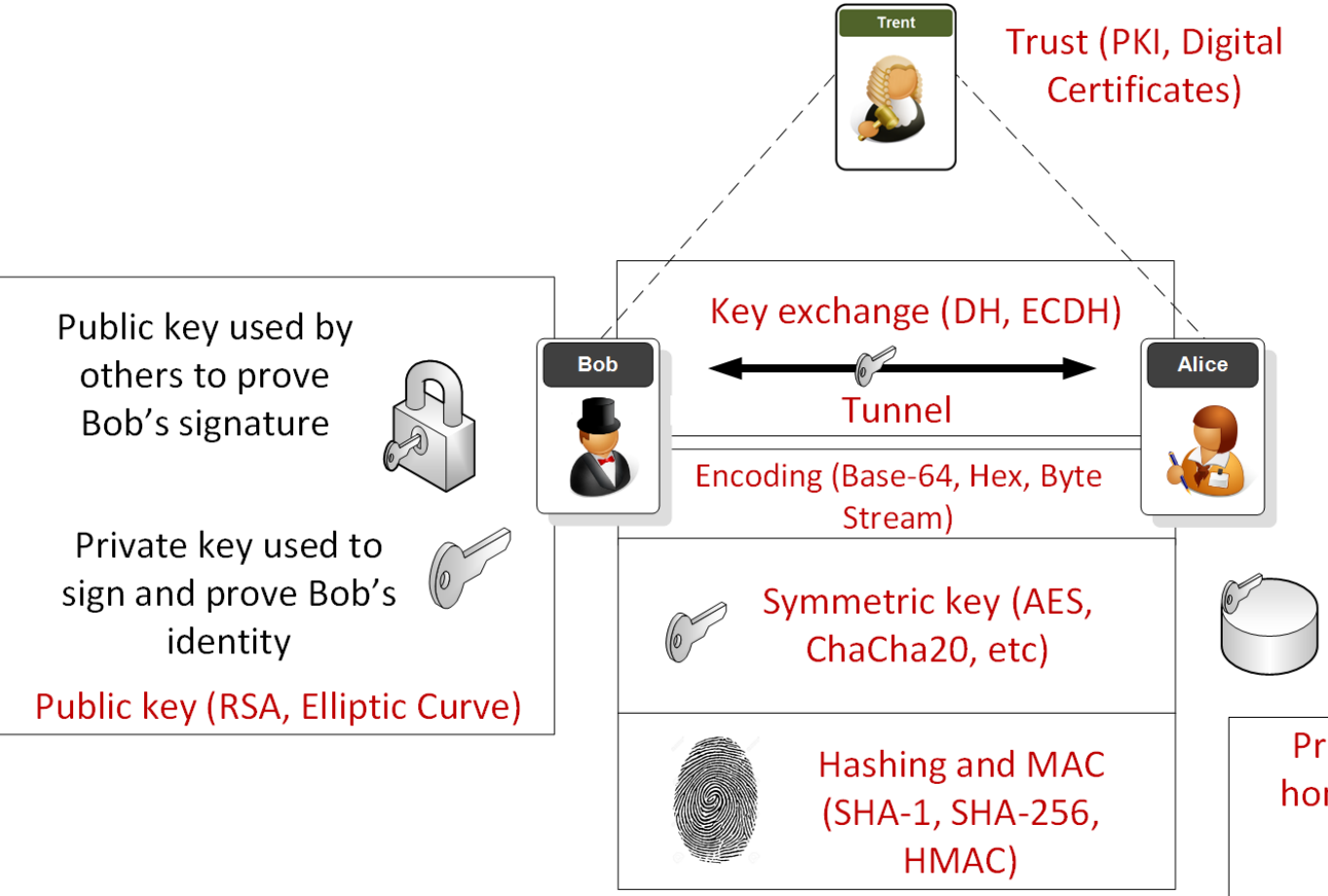
12-2pm: Lab (JKCC or Teams) – vSoc2, AWS or your own instance

6:30-7:30pm: Evening Session (Teams) - Recap

Draft Timetable

No	Date	Subject	Lab
2	26 Jan 2026	Ciphers and Fundamentals [Unit]	[Lab] [Demo]
3	2 Feb 2026	Symmetric Key [Unit]	[Lab] Vincent Rijmen
4	9 Feb 2026	Hashing and MAC [Unit]	[Lab] Ivan Damgård
5	16 Feb 2026	Asymmetric (Public) Key [Unit]	[Lab] Len Adleman
6	23 Feb 2026	Key Exchange [Unit]	[Lab] Whitfield Diffie
7	2 Mar 2026	Reading Week (Revision lecture)	Mini-project [Here] / Coursework
8	9 Mar 2026	Digital Signatures and Certificates [Unit]	[Lab]
9	16 Mar 2026	Test (Units 1-5) 40% of overall mark [Here]	
10	23 Mar 2026	Tunnelling [Unit]	[Lab Marty Hellman
11	13 Apr 2026	Blockchain [Unit]	[Lab] Troy Hunt
12	20 Apr 2026	Future Cryptography [Unit]	[Lab]
13	27 Apr 2026	Tokens, Authorization and Docker [Unit]	[Lab]
14	4 May 2026	Coursework Hand-in - 60% of overall mark (Sunday, 11 May 2026) [Coursework]	Daniel J Bernstein

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).

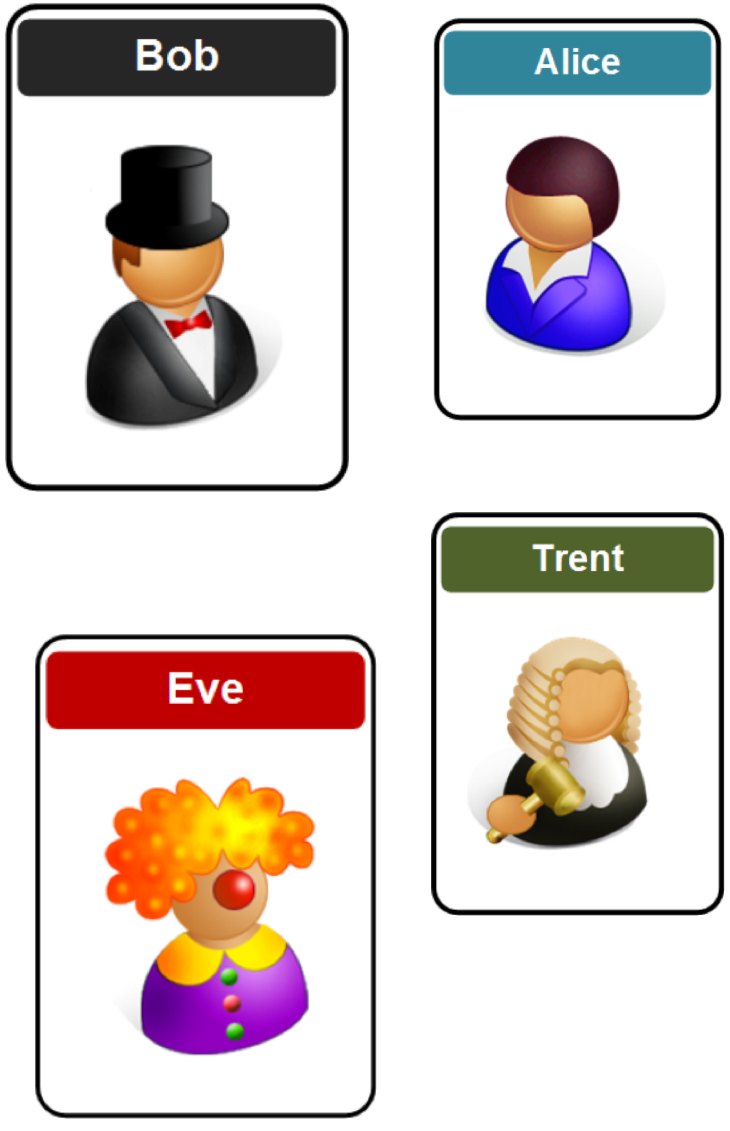
Prof Bill Buchanan OBE

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

2. Symmetric Key

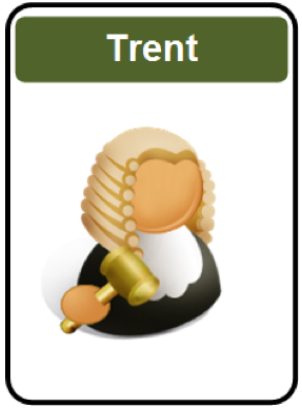
Basics
Block or Stream?
Secret Key Methods
Salting
AES
3DES
ChaCha20/Poly1305
Key Entropy

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

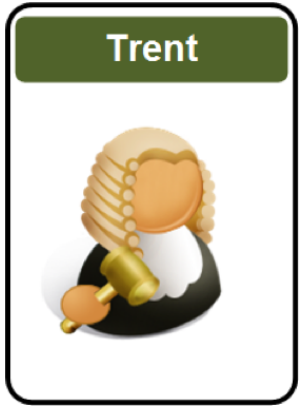
6. Signatures and Digital Certificates

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

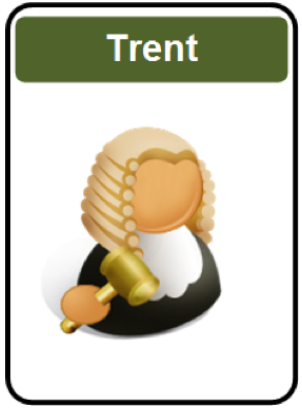
SSL/TLS.
Key generation/key exchange.
SSH.
IPSec.



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

8. Blockchain & Cryptocurrencies

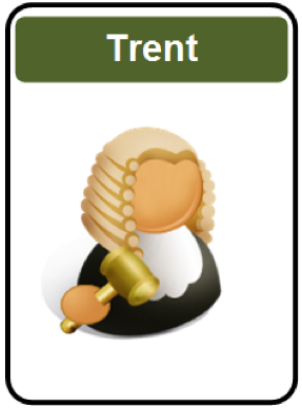
Principles.
Bitcoin.
Ethereum.
Smart Contracts.



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 FRSE

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 FRSE

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