Asymmetric Key

Basics
RSA/ECC
Applications (Encryption and Signing)

Prof Bill Buchanan OBE, FRSE
https://asecuritysite.com/rsa
https://asecuritysite.com/ecc
https://asecuritysite.com/elgamal

Asymmetric Key

Basics
RSA/ECC
Applications (Encryption and Signin

Prof Bill Buchanan OBE, FRSE
https://asecuritysite.com/rsa
https://asecuritysite.com/ecc
https://asecuritysite.com/elgamal

No	Date	Subject	La
2	18 Sept 2025	1. Introduction [Link] 2. Intrusion Detection Systems [Link]	Network Security Lab 1
3	25 Sept 2025	3. Network Security (Risks and Models) [Link]	Network Security Lab 2
4	2 Oct 2025	4. Ciphers and Fundamentals [Link]	AWS Security and Serv
5	9 Oct 2025	5. Secret Key 6. Hashing [Link]	Symmetric Key and Has
6	16 Oct 2025	7. Public Key [Link] 8. Key Exchange [Link]	Public Key and Key Excl
7	23 Oct 2025	Reading week/Revision session	Reading week/Cipher C
8	30 Oct 2025	9. Digital Certificates	Certificates Lab 6
9	6 Nov 2025	Test 1 here (6-8pm, JKCC)	
10	13 Nov 2025	10 Network Forensics here	Network Forensics Lab
11	20 Nov 2025	11. Splunk here	Splunk Lab Lab 8
12	27 Nov 2025	13. Tunnelling Here	Tunnelling Lab 9
13	4 Dec 2025	14. Blockchain and Cryptocurrencies here	Blockchain Lab. here
14	11 Dec 2025		
15	18 Dec 2025	Hand-in: TBC [Here]	

Asymmetri

Basics
RSA/ECC
Applications (Encryptior

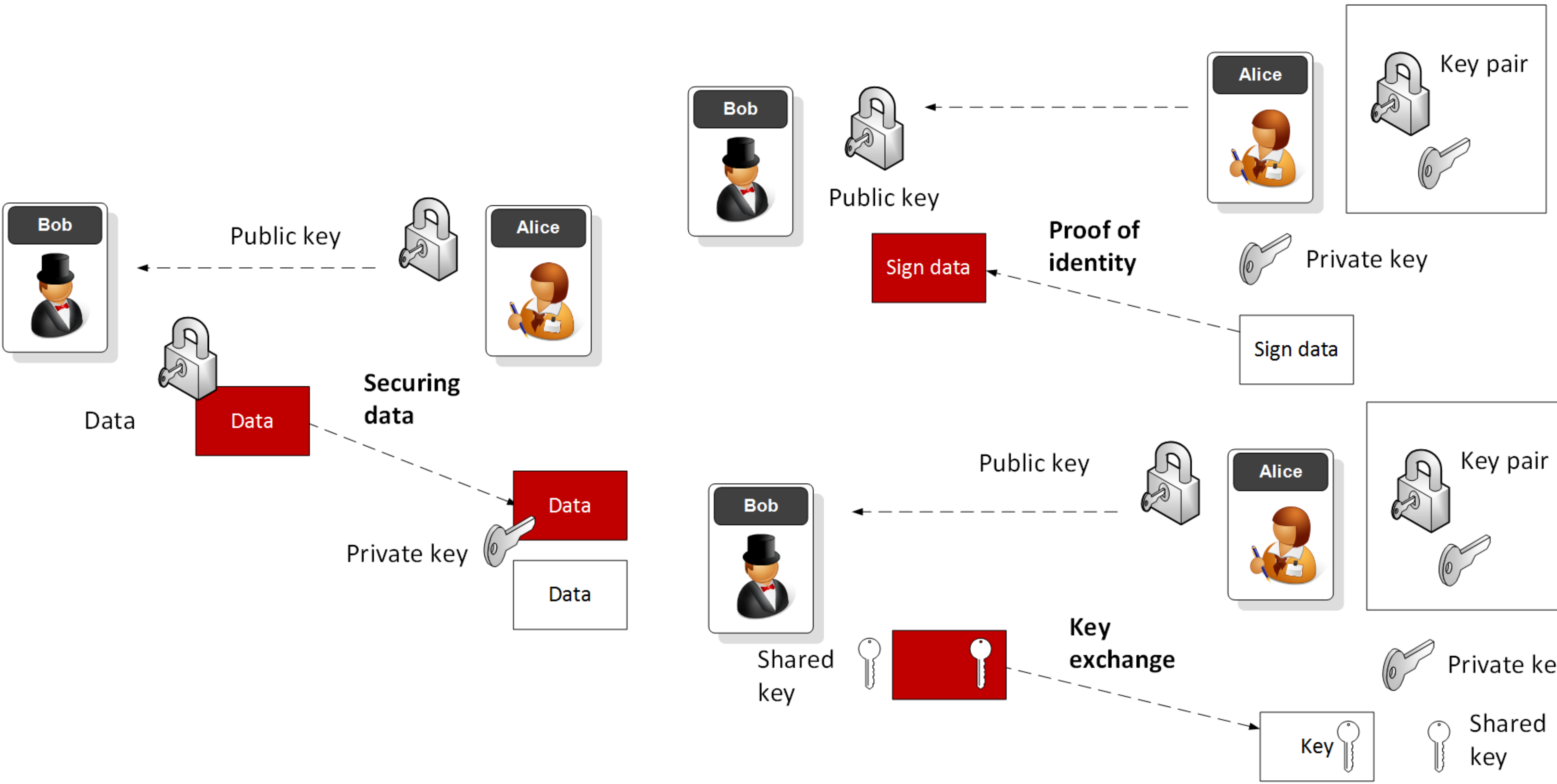
Prof Bill Buchanan OE
https://asecuritysite.cor
https://asecuritysite.cor
https://asecuritysite.cor

Coming Up...

Thu, 16 Oct 2025 09:00	**Network Security and Cryptography** MER_A17 PY-RG-WV
Thu, 16 Oct 2025 11:00	**Network Security and Cryptography** MER_JKCC_CLUSTER_11 JF-ML-OQ
Thu, 16 Oct 2025 11:00	**Network Security and Cryptography** MER_JKCC_CLUSTER_12 JM-XR-SZ
Thu, 16 Oct 2025 16:00	**Network Security and Cryptography** MER_JKCC_CLUSTER_09 QT-KI-ZO
Thu, 16 Oct 2025 16:00	**Network Security and Cryptography** MER_JKCC_CLUSTER_10 KR-TZ-PH
Thu, 16 Oct 2025 16:00	**Network Security and Cryptography** MER_JKCC_CLUSTER_13 BF-ER-SW

La
Security Lab 1
Security Lab 2
urity and Serv
ic Key and Has
y and Key Exc
week/Cipher C
es Lab 6
Forensics Lab
ab Lab 8
g Lab 9
in Lab. here

Public Key Methods

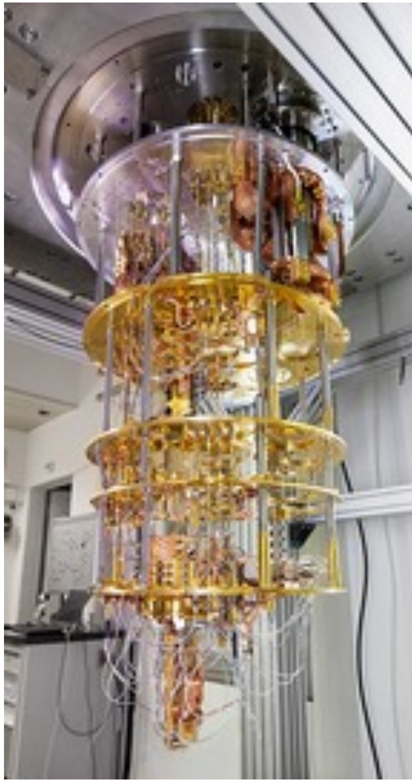


Public Key Methods

- **Integer Factorization**. Using prime numbers. Example: RSA. Key size: 2,048 bits (modulus). Signing, Digital Certificates.
- **Discrete Logarithms**. $Y = g^x \bmod P$. Example: ElGamal. Prime number size: 2,048 bits. Key handshake.
- **Elliptic Curve Relationships**. Example: Elliptic Curve. Private key: 256 bits. Public key: 512 bits. Bitcoin, IoT, Web, etc.

Public Key Methods

- **Integer Factorization**. Using prime numbers. Example: RSA. Key size: 2,048 bits (modulus). Signing, Digital Certificates.
- **Discrete Logarithms**. $Y = g^x \bmod P$. Example: ElGamal. Prime number size: 2,048 bits. Key handshake.
- **Elliptic Curve Relationships**. Example: Elliptic Curve. Private key: 256 bits. Public key: 512 bits. Bitcoin, IoT, Web, etc.



Public Key

RSA

Prof Bill Buchanan OBE

https://asecuritysite.com/rsa
https://asecuritysite.com/ecc
https://asecuritysite.com/elgamal

Eve

p

9,137,187,070,061,098,912,312,979,400,361
,251,189,847,923,809,497,258,114,688,790,
849,334,008,324,856,676,348,809,151,285,1
18,821,829,375,998,699,013,311,467,364,66
2,378,853,216,263,996,490,005,611,058,805

p

9,885,919,140,818,765,444,174,626,190,703
,294,219,553,850,295,249,705,938,896,539,
634,343,302,401,155,295,752,383,276,739,5
84,190,165,200,823,122,225,274,427,125,93
4,163,475,191,779,288,529,189,149,818,011

(p-1)*(q-1)

90,329,492,549,158,751,736,593,291,654,313,033,317,391,509,546,977,632,
830,551,342,194,781,230,803,832,847,247,315,213,556,011,813,523,182,777
,529,551,800,128,685,586,665,697,818,108,995,125,892,738,489,085,065,56
4,398,419,119,705,178,003,889,155,415,914,402,310,708,147,858,313,669,1
76,692,847,865,236,706,085,105,432,191,429,510,583,595,108,030,256,069,
207,938,161,732,170,083,525,341,774,967,620,008,260,040

Eve

With Diffie-Hellman we need the other side to be active before we send data. Can we generate a special one-way function which allows is to distribute an encryption key, while we have the decryption key?

Bob

Alice

Encryption/ Decryption → Communications Channel → Encryption/ Decryption

Solved in 1977, By Ron Rivest, Adi Shamir, and Len Aldeman created the RSA algorithm for public-key encryption.

Public Key Methods

Public Key

RSA

Pick p and q (two large primes)

$N = p.q$

$PHI = (p-1)(q-1)$

Pick e (no factors with PHI)

$d = InvMod(e, PHI)$

Public: (e,N)
Private: (d,N)

$C = M^e \pmod N$
$P = C^d \pmod N$

ElGamal

Pick random value x, generator (g) and prime (p)

$Y = g^x \pmod p$

Public key: (Y,p)
Private: (x,p)

ECC

Pick random value sk and curve (a, b, G, p, o). G is the base point on curve, p is a prime number, and o is the order of the curve).

For example: $y^2=x^3 + ax + b \pmod p$

$Pk = sk.G$

Public key: Pk
Private key: sk

RSA

- Two primes p, q.
- Calculate N (modulus) as p x q eg 3 and 11. n=33.
- Calculate PHI as (p-1)x(q-1). PHI=20
- Select e for no common factor with PHI. e=3.
- Encryption key [e,n] or [3,33].
- (d x e) mod 20 = 1
- (d x 3) mod 20 = 1
- d= 7
- Decryption key [d,n] or [7,33] (link)

Calc

Example

RSA

- Encryption key [e,n] or [3,33].
- Decryption key [d,n] or [7,33]
- Cipher = M^e mod N

eg M=5.

- Cipher = 5^3 mod 33 = 26
- Decipher = C^d mod N
- Decipher = $(26)^7$ mod 33 = 5

Public Key

Basics

RSA

Applications (Encryption and Signing)

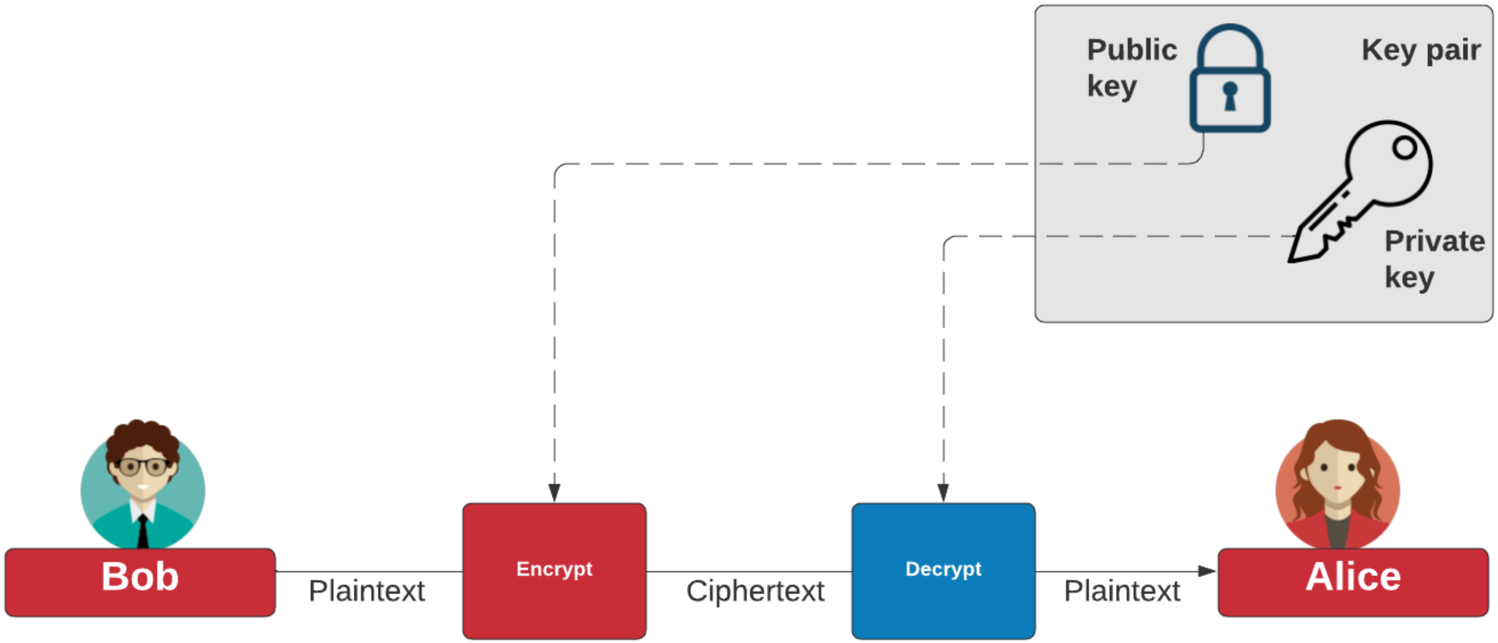
Prof Bill Buchanan OBE

https://asecuritysite.com/rsa

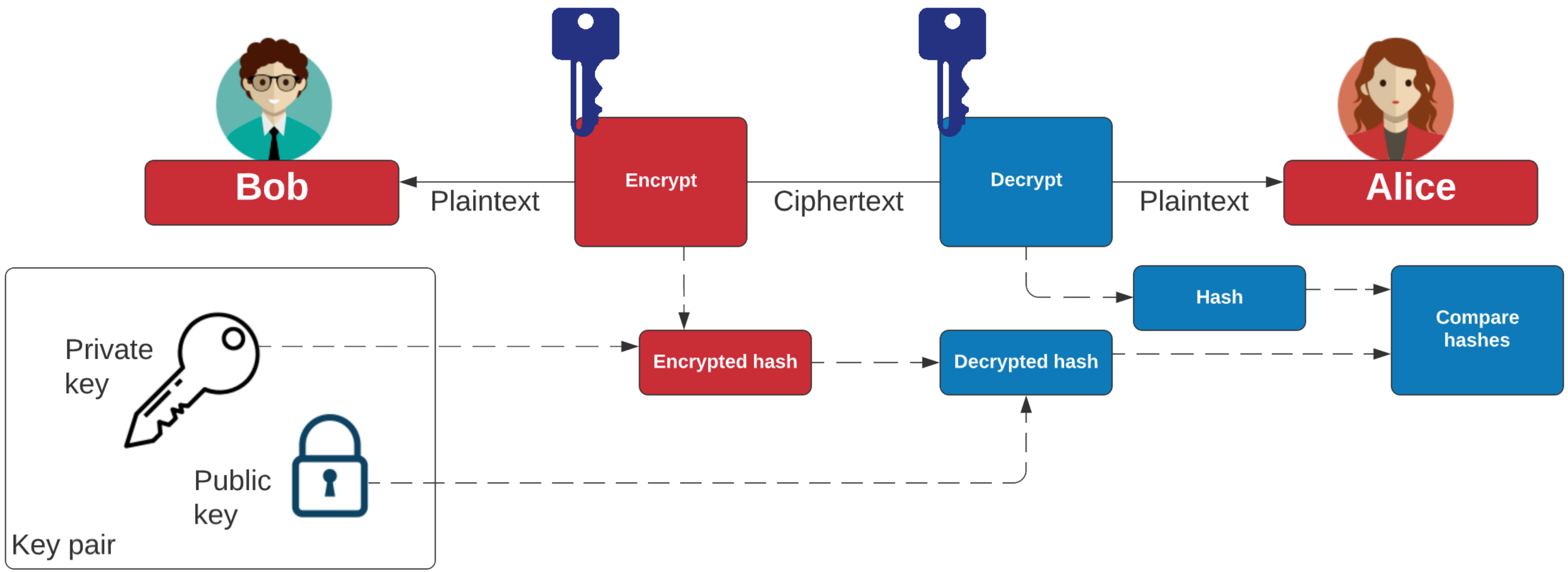
https://asecuritysite.com/ecc

https://asecuritysite.com/elgamal

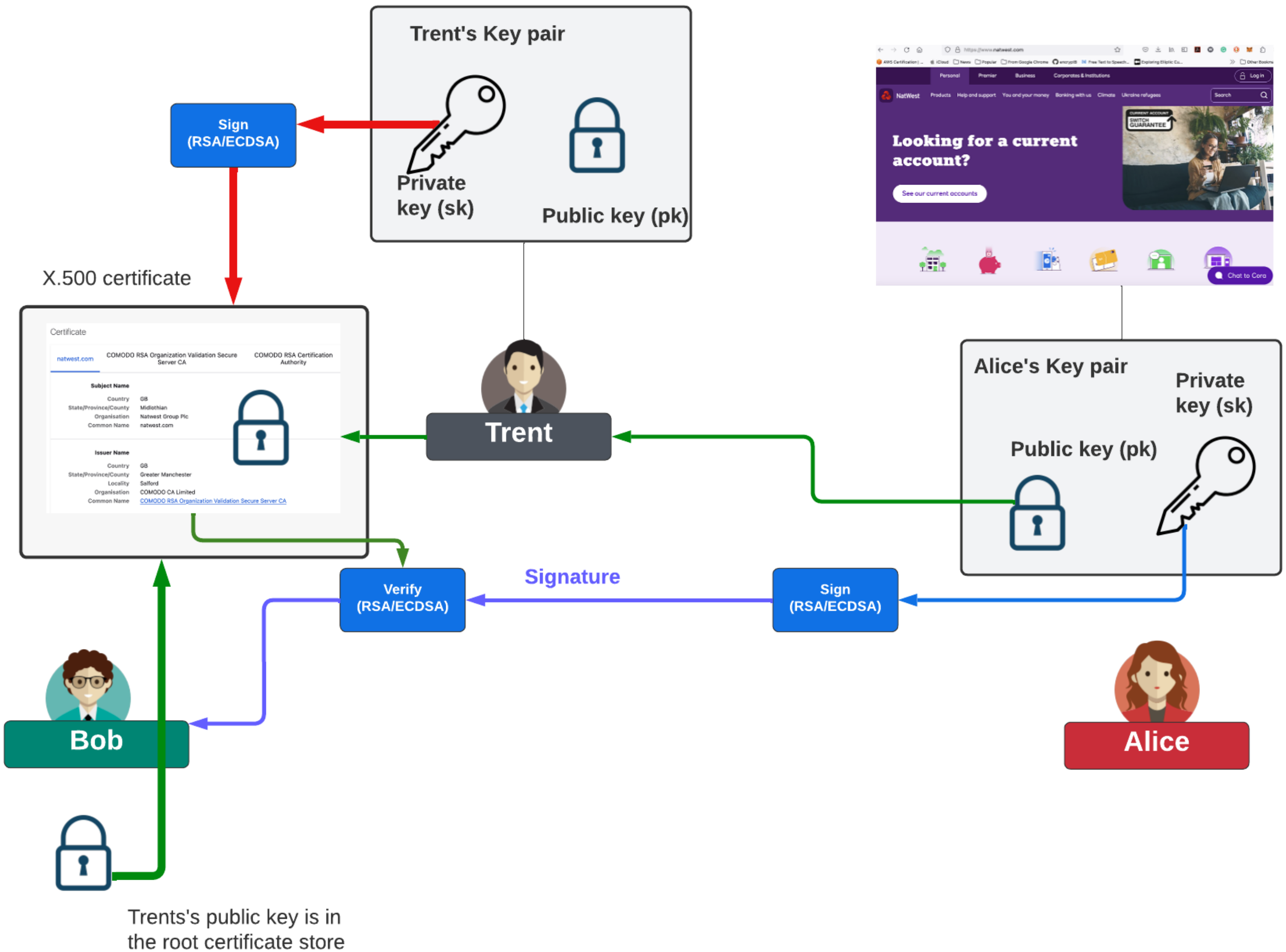
Public Key Encryption



Public Key Digital Signing



Public Key Digital Signing



Public Key

Basics
RSA
Applications (Encryption and Signing)

Prof Bill Buchanan OBE

https://asecuritysite.com/rsa
https://asecuritysite.com/ecc
https://asecuritysite.com/elgamal