

Discrete logarithms within computer and network security

Prof Bill Buchanan, Edinburgh Napier

<http://asecuritysite.com> @billatnapier

Introduction.

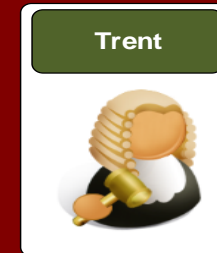
Encryption:

- Public/Private Key.
- Key Exchange.

Authentication.

Signatures.

ElGamal.



Discrete logarithms within computer and network security

Prof Bill Buchanan, Edinburgh Napier

<http://asecuritysite.com> @billatnapier

Introduction.

Encryption:

- Public/Private Key.
- Key Exchange.

Authentication.

Signatures.

ElGamal.



Introduction

Bruce Schneier



Twofish,
Blowfish, Secret
and

Vincent Rijmen
and Joan Daemen



AES

Modern private
key encryption

Rivest, Shamir
& Aldeman



Public-key
encryption

Ron
Rivest



Hashing

Phil
Zimmerman



PGP
Encryption

Whitfield
Diffie



Key
interchange

Introduction

Encryption



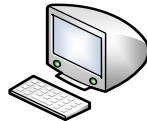
Intruder

Eve

Privacy (Private Key)
Identity (Public Key)
Integrity (Public/Private Key)



Bob



Alice



John



Trent

Trusted third party



Bob

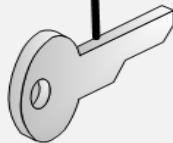


Eve

The major problem is that Eve could gain the encoding algorithm.

Hello

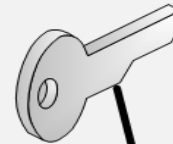
Standard
Encryption
Algorithm



H&\$d.

Communications
Channel

H&\$d.



Hello

Standard
Encryption
Algorithm

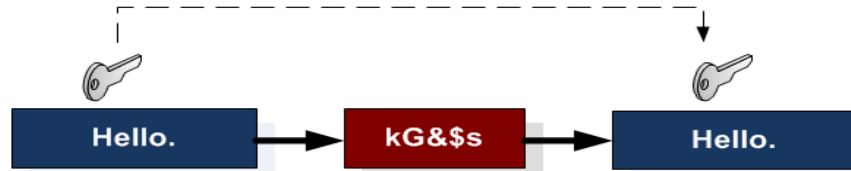


Alice





Bob



Symmetric encryption



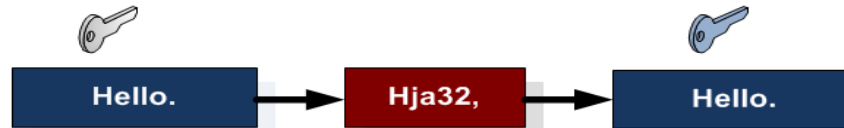
Alice

Private-key

Private-key:
RC2, RC4,
DES, 3DES,
AES



Bob



Asymmetric encryption



Alice

Public-key

Public-key:
RSA, DSA
(factoring prime
numbers)
FIPS 186-2,
ElGamal
(Elliptic curve)



Bob



One-way hash



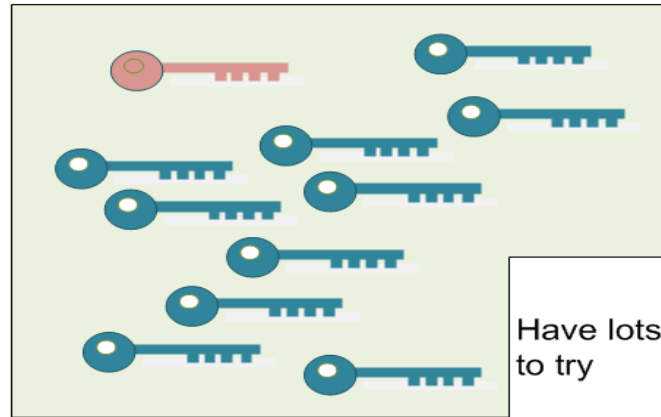
Alice

Hashing

Hashing:
MD5, SHA-1

Strength: 80-bit
DES -> 1024 RSA
-> 160 bit Elliptic





Have lots of different things to try

13,407,807,929,942,597,099,574,02
4,998,205,846,127,479,365,820,592,
393,377,723,561,443,721,764,030,0
73,546,976,801,874,298,166,903,42
7,690,031,858,186,486,050,853,753,
882,811,946,569,946,433,649,006,0
84,096



Make it mathematically
difficult ... prime numbers
... and large number maths

Bob



Alice



Trent



Eve



Number of keys

The larger the key, the greater the key space.

Code size	Number of keys	Code size	Number of keys	Code size	Number of keys
1	2	12	4,096	52	4.5×10^{15}
2	4	16	65,536	56	7.21×10^{16}
3	8	20	1,048,576	60	1.15×10^{18}
4	16	24	16,777,216	64	1.84×10^{19}
5	32	28	2.68×10^8	68	2.95×10^{20}
6	64	32	4.29×10^9	72	4.72×10^{21}
7	128	36	6.87×10^{10}	76	7.56×10^{22}
8	256	40	1.1×10^{12}	80	1.21×10^{24}
9	512	44	1.76×10^{13}	84	1.93×10^{25}
10	1024	48	2.81×10^{14}	88	3.09×10^{26}



Discrete logarithms within computer and network security

Prof Bill Buchanan, Edinburgh Napier

<http://asecuritysite.com> @billatnapier

Introduction.

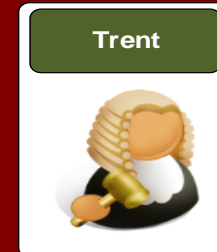
Encryption:

- Public/Private Key.
- Key Exchange.

Authentication.

Signatures.

ElGamal.



Encryption

Codes and Secrets

One Way Hash

Bob



Alice



Eve



Trent





**Hashing
Algorithm (MD5)**
- 128 bit signature



hello

XUFAKrxLKna5cZ2REBfFkg

Hello

ixqZU8RhEpaoJ6v4xHgE1w

Hello. How are you?

CysDE5j+zOUbCYztTdsFiw

Napier

j4NXH5Mkrk4j13N1MFXHtg

Base-64

hello

5D41402ABC4B2A76B9719D911017C592

Hello

8B1A9953C4611296A827ABF8C47804D7

Hello. How are you?

CC708153987BF9AD833BEBF90239BF0F

Napier

8F83571F9324AE4E23D773753055C7B6

Hex

Codes and Secrets

Private Key

Bob



Alice



Eve



Trent





Bob



Eve

The major problem is that Eve could gain the encoding algorithm.

Hello

Standard
Encryption
Algorithm

Communications
Channel

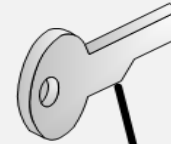
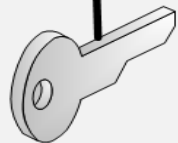
Standard
Encryption
Algorithm

Hello

H&\$d.

H&\$d.

Alice

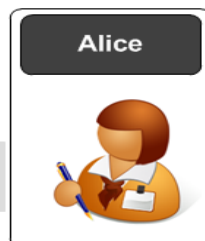




Bob

Hello. How are you?

kG&\$s &FDsaf *fd\$



Alice



Eve

kG&\$s &FDsaf *fd\$

A major problem in encryption is playback where an intruder can copy an encrypted message and play it back, as the same plain text will always give the same cipher text.



The solution is to add **salt** to the encryption key, as that it changes its operation from block-to-block (for block encryption) or data frame-to-data frame (for stream encryption)



Block 1

- DES/3DES – 64 bits
- RC2 – 64 bits
- AES/Rijndael – 128 bits

Block 2

- DES/3DES – 64 bits
- RC2 – 64 bits
- AES/Rijndael – 128 bits

Electronic Code Book (ECB)

method. This is weak, as the same cipher text appears for the same blocks.

Hello → 5ghd%43f=

Hello → 5ghd%43f=



Encrypted
Block

Encrypted
Block

Block 1

- DES/3DES – 64 bits
- RC2 – 64 bits
- AES/Rijndael – 128 bits

Block 2

- DES/3DES – 64 bits
- RC2 – 64 bits
- AES/Rijndael – 128 bits

Adding salt. This is typically done with an IV (Initialisation Vector) which must be the same on both sides. In WEP, the IV is incremented for each data frame, so that the cipher text changes.



IV

Encrypted
Block

Encrypted
Block

Codes and Secrets

Passing Keys

Bob



Alice



Eve



Trent



Eve



Private key

Private key uses the same key for encryption and decryption ... how does Bob send the key to Alice?

How do Bob and Alice send their private (secret) key without Eve getting it?

Hello

Encryption

Communications Channel

Decryption

Hello

H&\$d.

H&\$d.

Bob



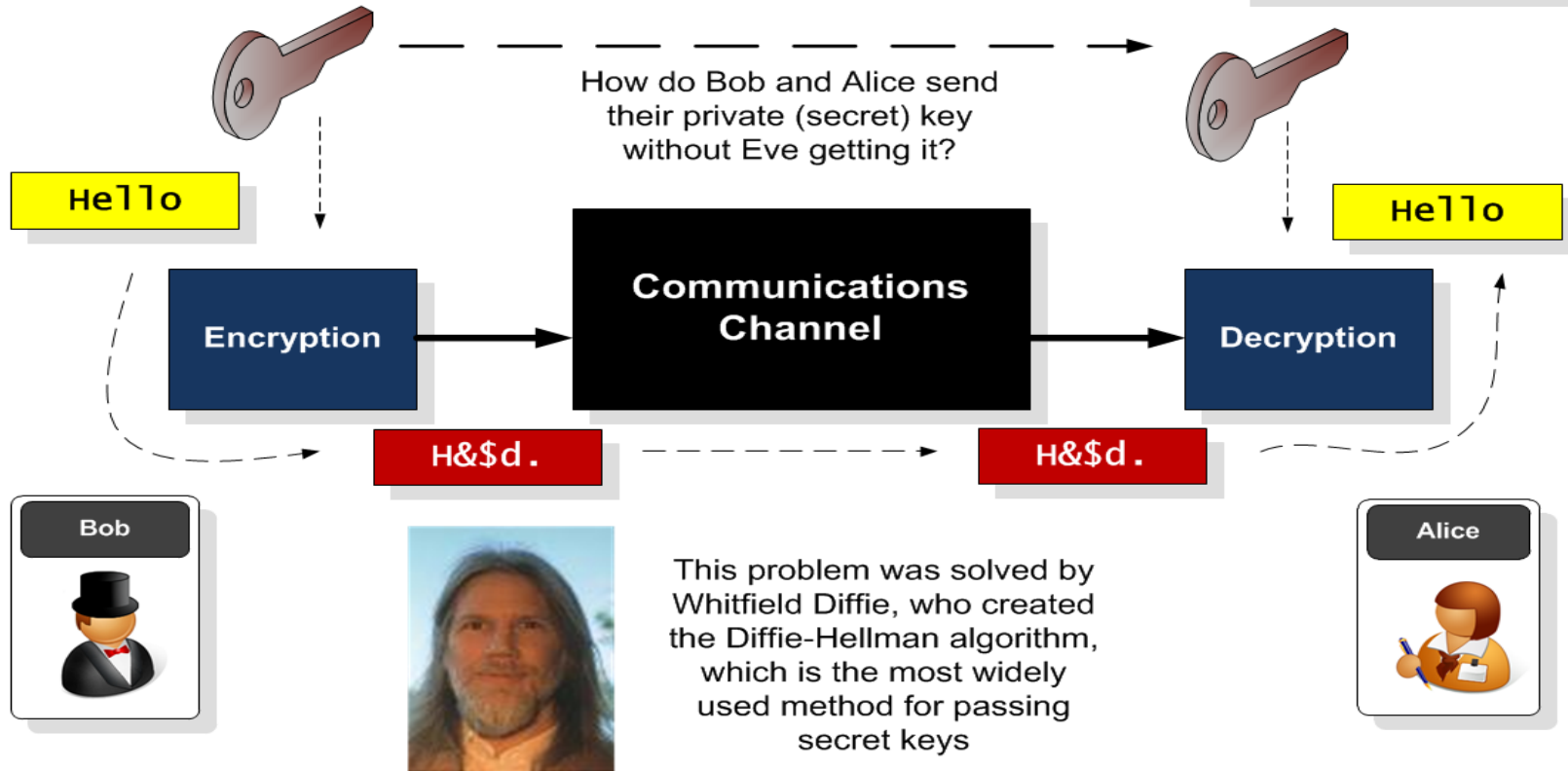
Alice





Diffie-Hellman

One of the most widely method for creating a secret key which is the same for Bob and Alice





Diffie-Hellman

Eve can listen to the values of A and B , but should not be able to determine the secret key

1. Both nodes agree on two values (G and n)

2. Generate a random value (x)

2. Generate a random value (y)

3. $A = G^x \bmod n$

3. $B = G^y \bmod n$

5. $K1 = B^x \bmod n$

4. A and B
values
exchanged

5. $K2 = A^y \bmod n$

$K1$ and $K2$ should be the **same** and are the secret key

John





Diffie-Hellman

Eve can listen to the values of A and B, but should not be able to determine the secret key

1. Both nodes agree on two values (5 and 7)

2. Generate a random value (2)

2. Generate a random value (3)

$$3. A = 5^2 \bmod 8 = 25 \bmod 7 = 4$$

$$3. B = 5^3 \bmod 7 = 125 \bmod 7 = 6$$

4. A and B values exchanged

$$5. K1 = 6^2 \bmod 7 = 36 \bmod 7 = 1$$

$$5. K2 = 4^3 \bmod 7 = 64 \bmod 7 = 1$$

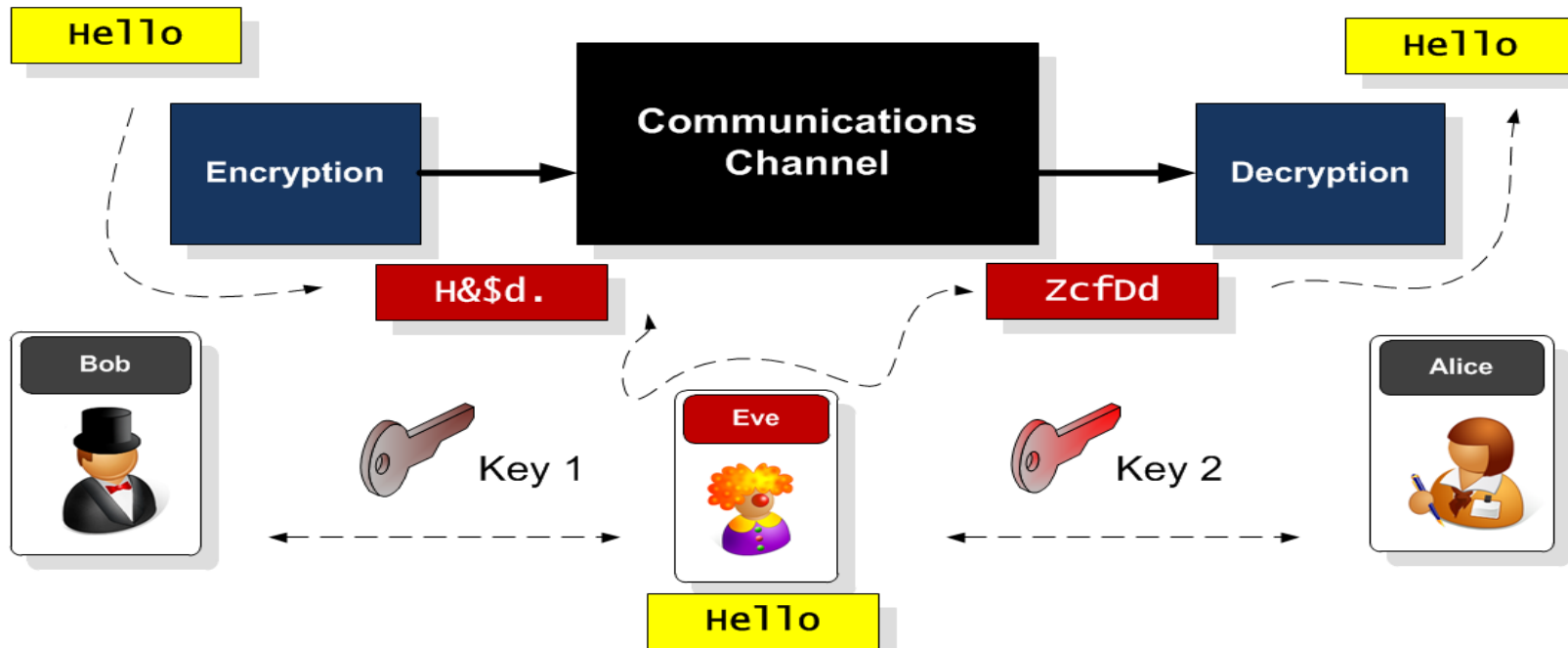
K1 and K2 should be the **same** and are the secret key



Diffie-Hellman suffers from a man-in-the-middle attack, where Eve negotiates for each side, and creates two encryption channels

Man-in-the-middle

Diffie-Hellman suffers from Eve intercepting the key interchange, so that Bob thinks he's talking to Alice for the key exchange.



Codes and Secrets

Public Key

Bob



Alice



Eve



Trent





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





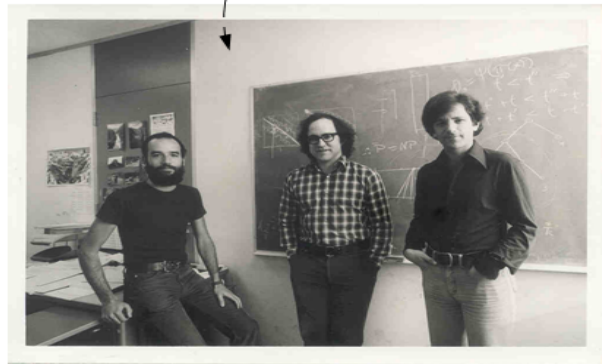
With Diffie-Hellman we need the other side to be active before we send data. Can we generate a special one-way function which allows us to distribute an encryption key, while we have the decryption key?



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 generates two keys: A public key and a private one. These are special in that if one is applied to encrypt, the other can be used to decrypt

Public-key

Public key are keys which relate to extremely large prime numbers (as it is difficult to factorise large prime numbers). It is extremely difficult to determine a private key from a public key.



Encryption

Communications
Channel

Decryption



Public Key



Private Key

Public Key



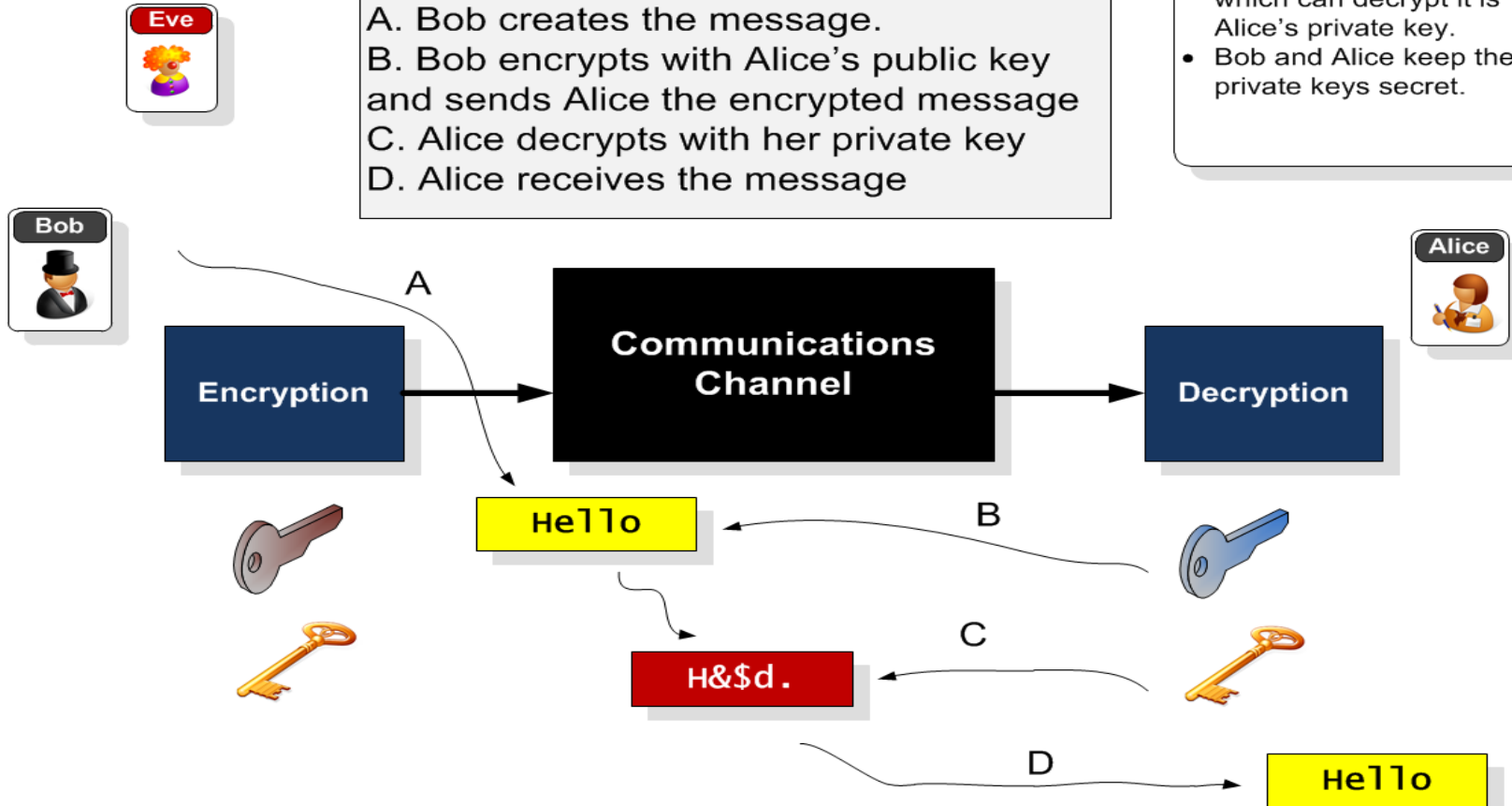
Private Key

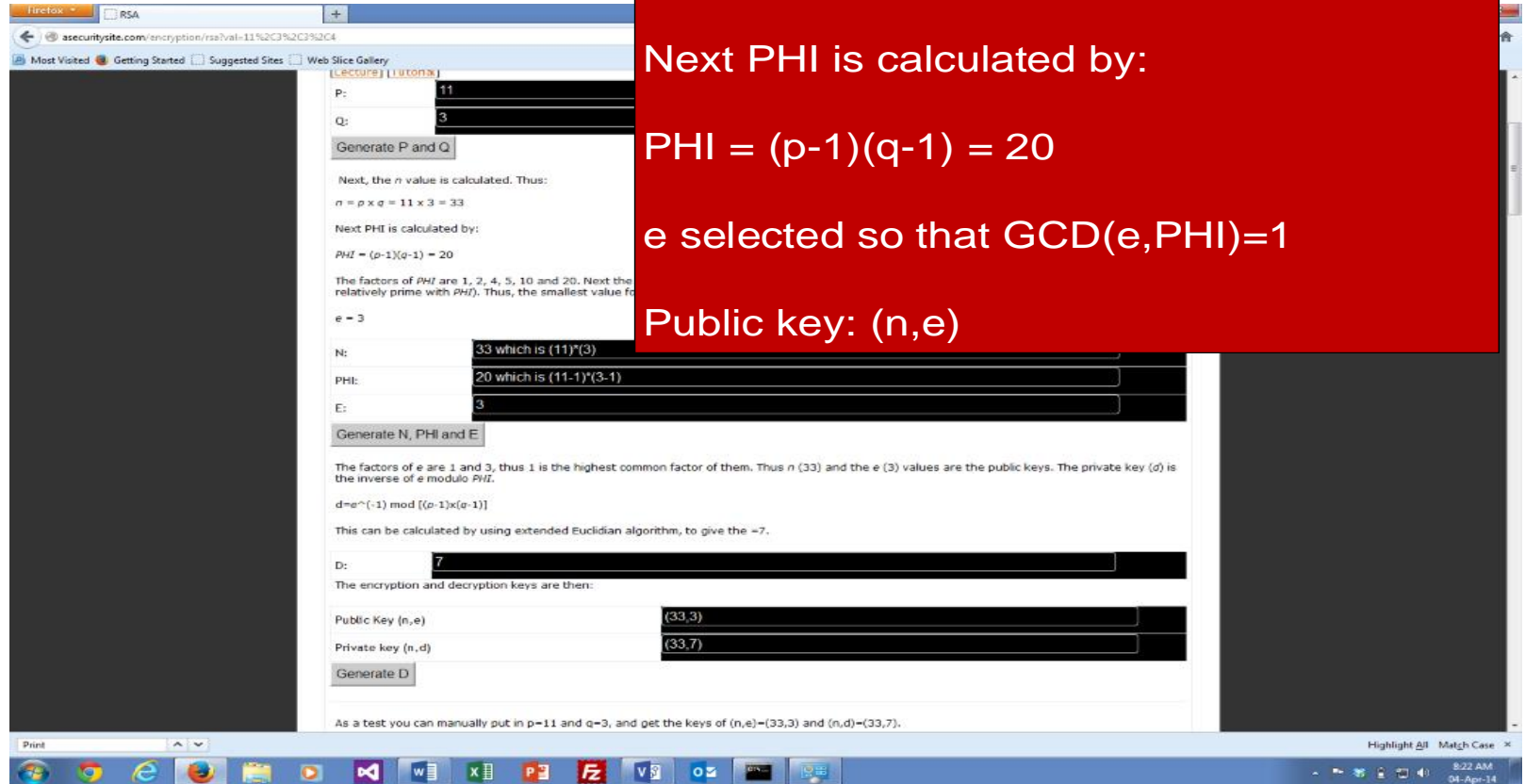


Public-key

- Once Bob encrypts the message, the only key which can decrypt it is Alice's private key.
- Bob and Alice keep their private keys secret.

A. Bob creates the message.
B. Bob encrypts with Alice's public key and sends Alice the encrypted message
C. Alice decrypts with her private key
D. Alice receives the message





The screenshot shows a web browser window with the URL `asecuritysite.com/encryption/rse/val=11%2C3%2C3%2C4`. The page content includes the following steps:

- Generate P and Q:** P: 11, Q: 3. The button "Generate P and Q" is clicked.
- Next, the n value is calculated. Thus:** $n = p \times q = 11 \times 3 = 33$
- Next PHI is calculated by:** $PHI = (p-1)(q-1) = 20$
- The factors of PHI are 1, 2, 4, 5, 10 and 20. Next the relatively prime with PHI. Thus, the smallest value for e = 3**
- Generate N, PHI and E:** The button "Generate N, PHI and E" is clicked.
- The factors of e are 1 and 3, thus 1 is the highest common factor of them. Thus n (33) and the e (3) values are the public keys. The private key (d) is the inverse of e modulo PHI.**
- d = e⁻¹ mod [(p-1)(q-1)]**
- This can be calculated by using extended Euclidian algorithm, to give the =7.**
- The encryption and decryption keys are then:**
- Public Key (n,e):** (33,3)
- Private key (n,d):** (33,7)
- Generate D:** The button "Generate D" is clicked.
- As a test you can manually put in p=11 and q=3, and get the keys of (n,e)=(33,3) and (n,d)=(33,7).**

Select two primes (p,q)

Next, the n value is calculated. Thus:

$$n = p \times q = 11 \times 3 = 33$$

Next PHI is calculated by:

$$PHI = (p-1)(q-1) = 20$$

e selected so that $GCD(e, PHI) = 1$

Public key: (n,e)

Discrete logarithms within computer and network security

Prof Bill Buchanan, Edinburgh Napier

<http://asecuritysite.com> @billatnapier

Introduction.

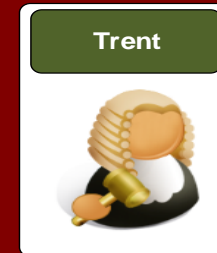
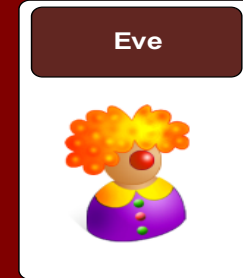
Encryption:

- Public/Private Key.
- Key Exchange.

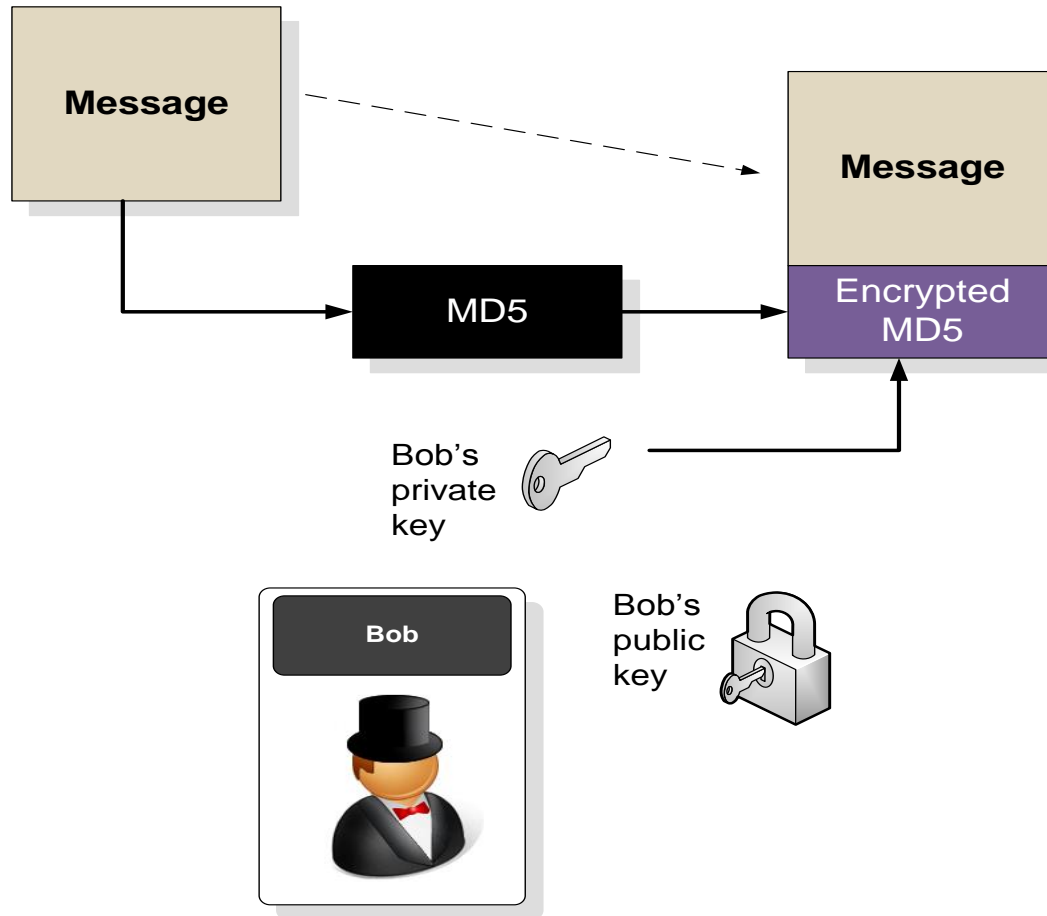
Authentication.

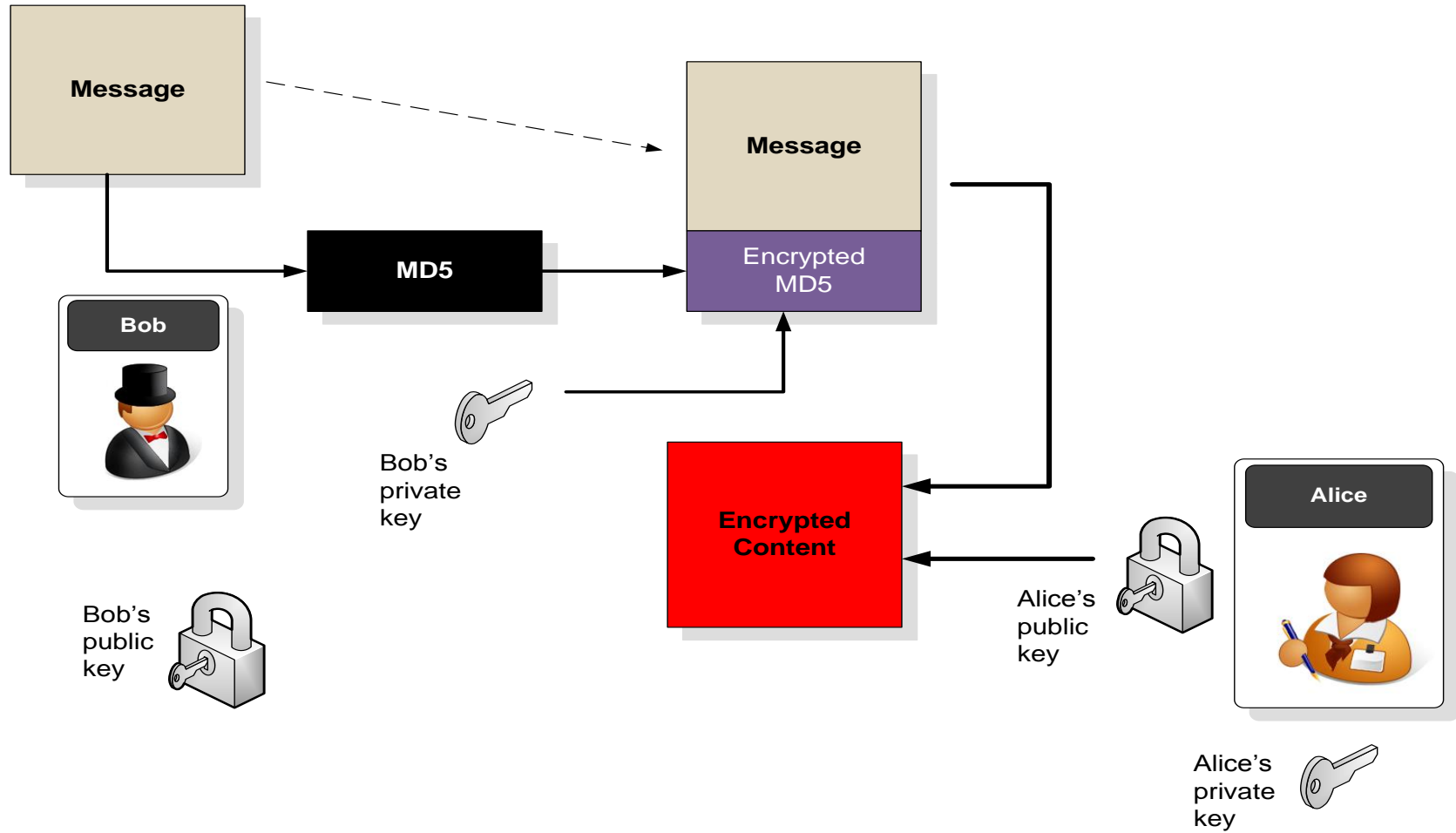
Signatures.

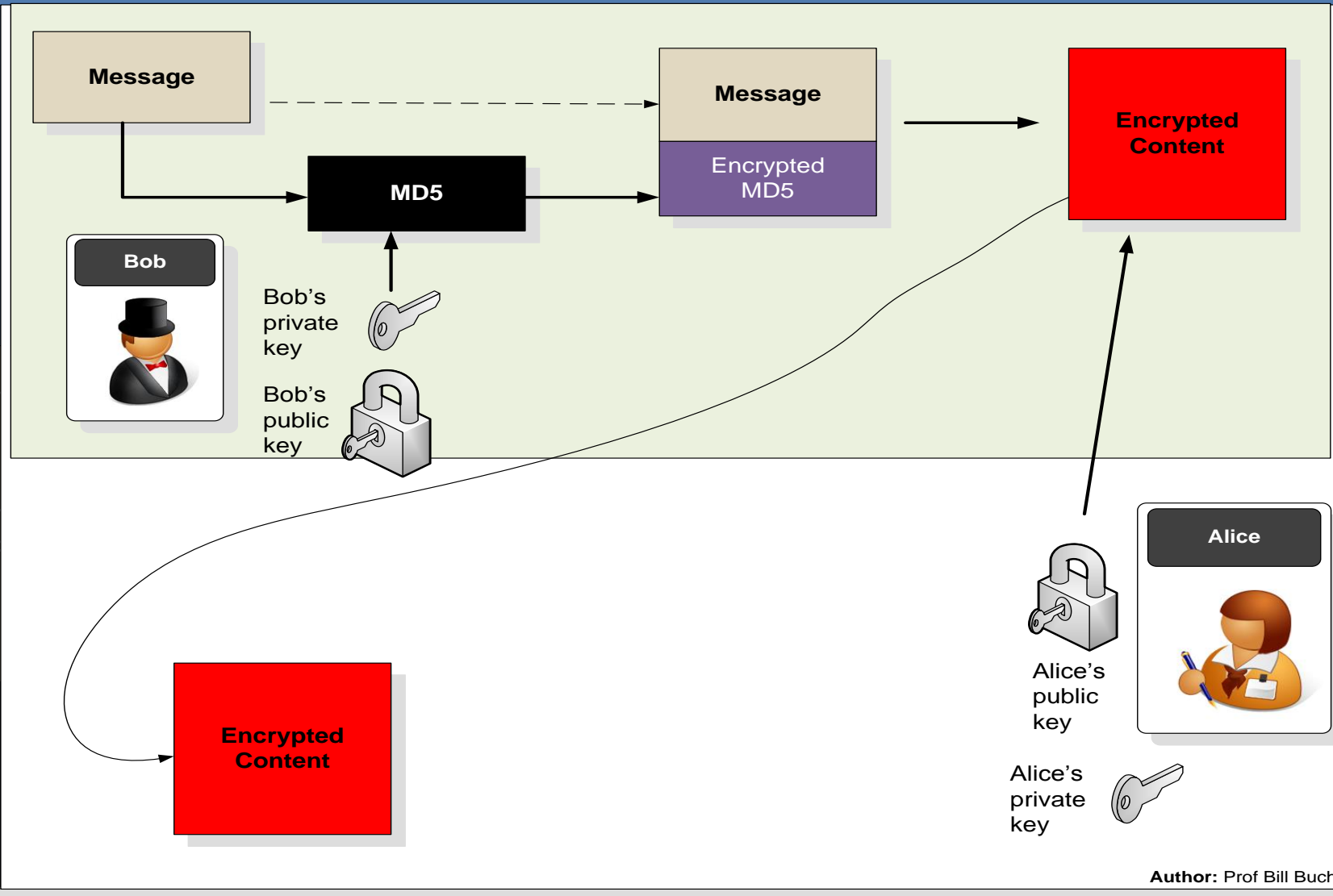
ElGamal.



Authentication

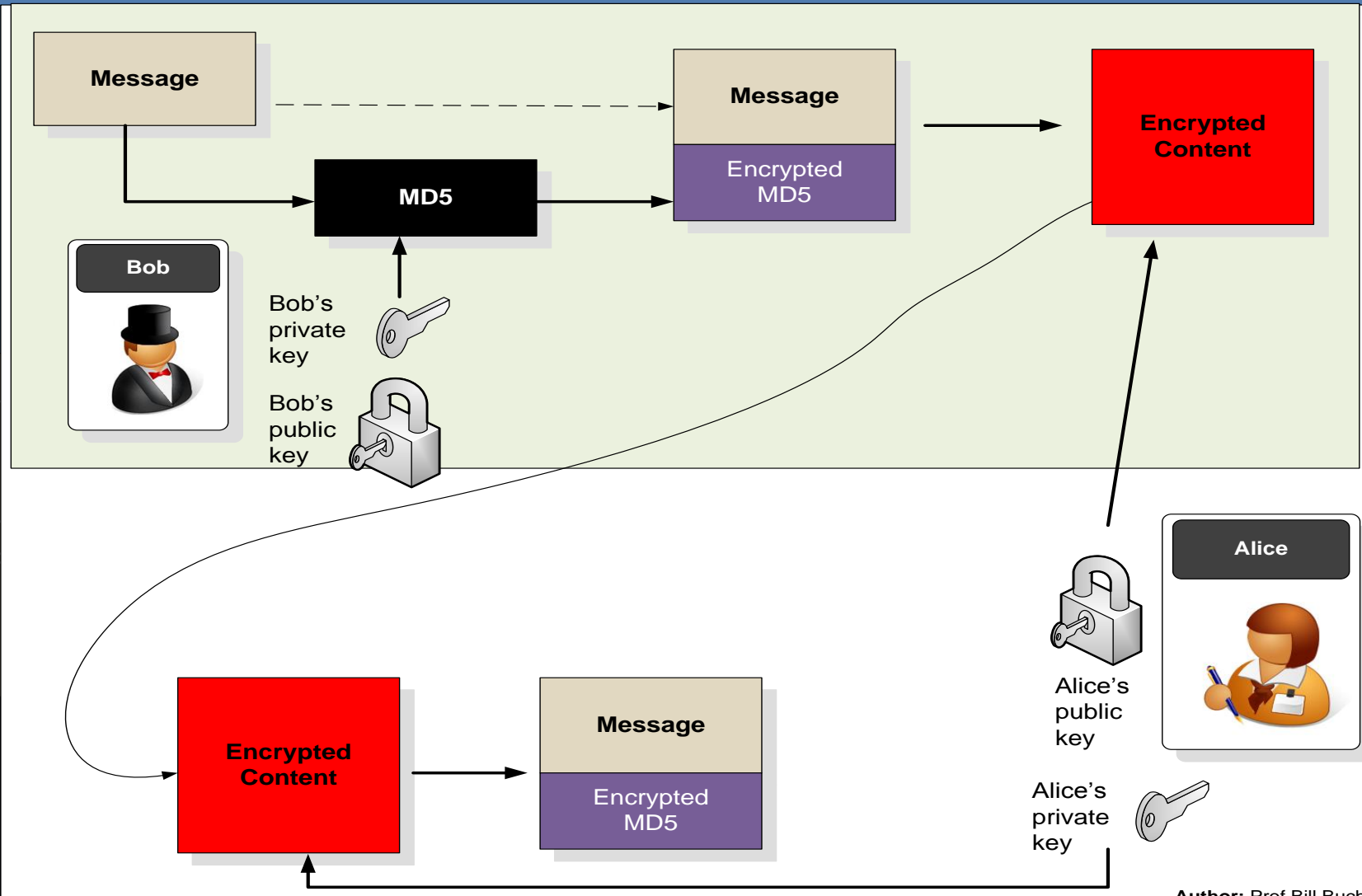






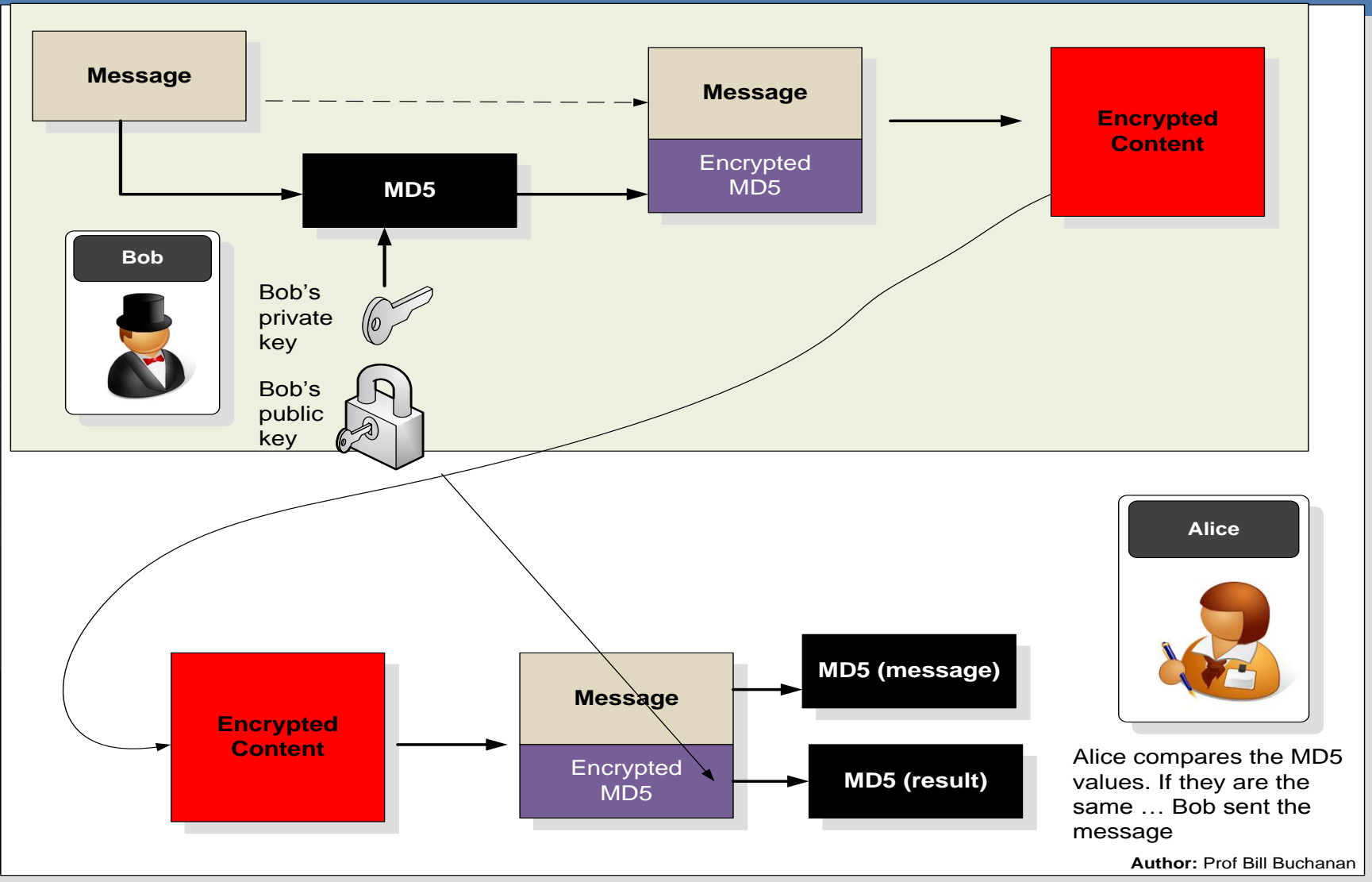
Authentication

The magic private key



Author: Prof Bill Buchanan

Alice decrypts the message



Alice compares the MD5 values. If they are the same ... Bob sent the message

Author: Prof Bill Buchanan

Discrete logarithms within computer and network security

Prof Bill Buchanan, Edinburgh Napier

<http://asecuritysite.com> @billatnapier

Introduction.

Encryption:

- Public/Private Key.
- Key Exchange.

Authentication.

Signatures.

ElGamal.



ElGamal



$$Y = g^x \text{ mod } p$$



Extremely difficult to the value of x , and there can be many solutions



$$Y = 3^4 \text{ mod } 17 \rightarrow 13$$





First Bob generates a prime number (p) and a number (g) which is between 1 and ($p-1$):

P:

G:

Bob select a random number (x) which will be his private key:

Bob selects a random number(x):

He then calculates Y :

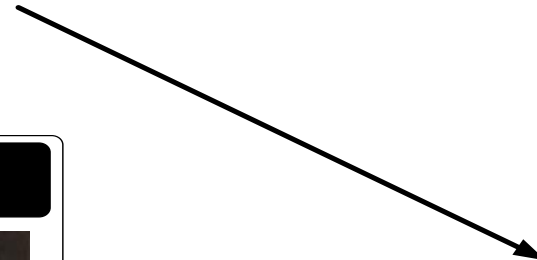
Bob sends g , p and Y to Alice.

p

g

x

$$Y = g^x \bmod p$$





p

g

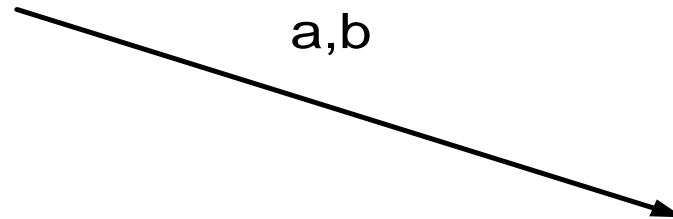
y

M (message)

K (random)

$a = g^k \text{ mod } P$

$b = y^k \text{ M mod } P$



a,b





Typical application:

Diffie-Hellman used to generate private-key.
Public-key used for authentication.
Private-key used for encryption.



Encryption/
Decryption

Communications
Channel

Encryption/
Decryption



Key exchange (Diffie-Hellman)



Secret key used to encrypt/decrypt
(DES/3DES/AES)

Public key



Used to authenticate (RSA)

Private key



RSA 2048 bits
Replace by:
ElGamal 160bits



Private key



Public key

Discrete logarithms within computer and network security

Prof Bill Buchanan, Edinburgh Napier

<http://asecuritysite.com> @billatnapier

Introduction.

Encryption:

- Public/Private Key.
- Key Exchange.

Authentication.

Signatures.

ElGamal.

