Chapter 4: Public Key

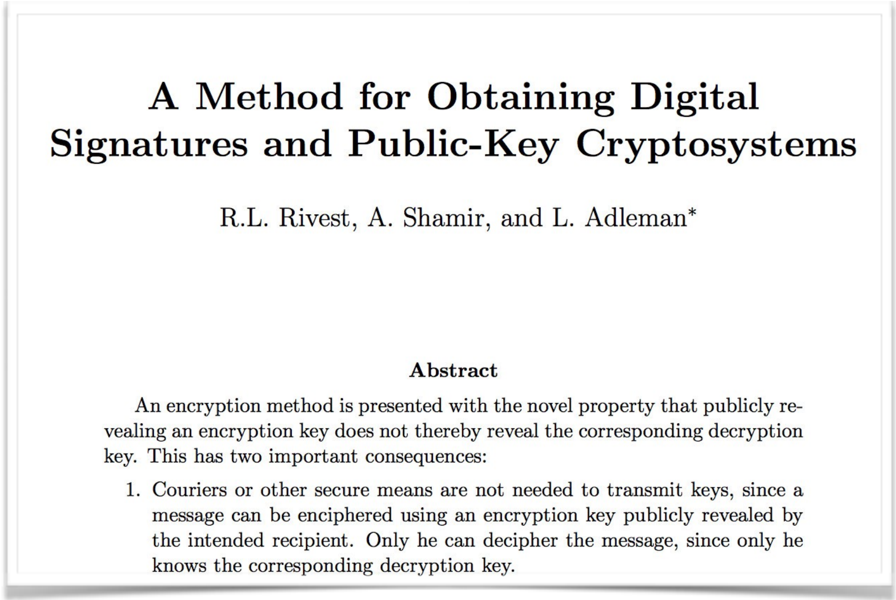
Prof Bill Buchanan OBE

http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption

Bruce


INTERNATIONAL BESTSELLER
Over 150,000 copies sold in hardcover
Secrets & Lies
Digital Security in a Networked World
With new information about post-9/11 security
Bruce Schneier

Bruce



A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

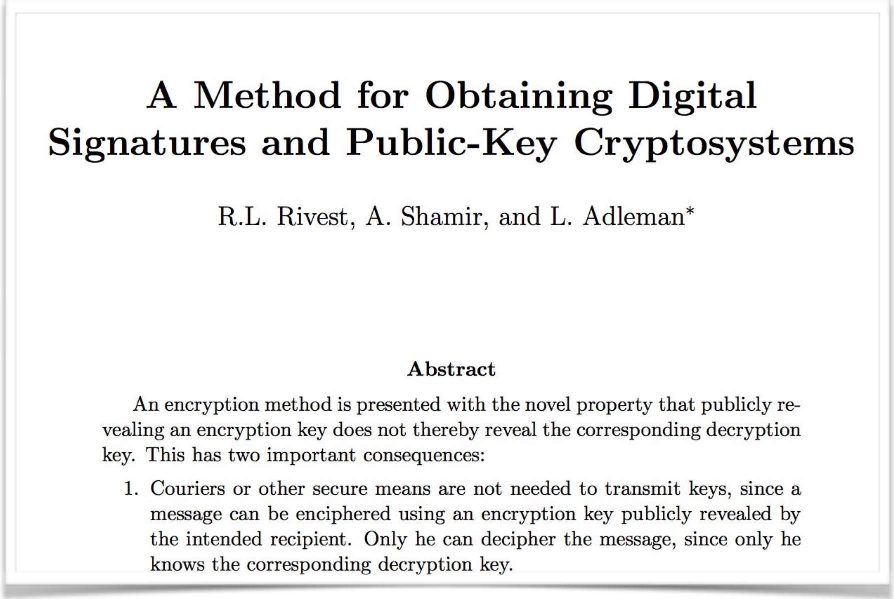
R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

Bruce



A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

Bruce

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

Table 1

Digits	*Number of operations*	*Time*
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^{9} year
300	1.5×10^{29}	4.9×10^{15} yea
500	1.3×10^{39}	4.2×10^{25} yea

Bruce

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

Table 1

Digits	*Number of operations*	*Time*
50	1.4×10^{10}	3.9 hours
75	9.0×10^{12}	104 days
100	2.3×10^{15}	74 years
200	1.2×10^{23}	3.8×10^{9} year
300	1.5×10^{29}	4.9×10^{15} yea
500	1.3×10^{39}	4.2×10^{25} yea

For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem. We will distinguish their encryption and decryption procedures with subscripts: E_A, D_A, E_B, D_B.

Table 1

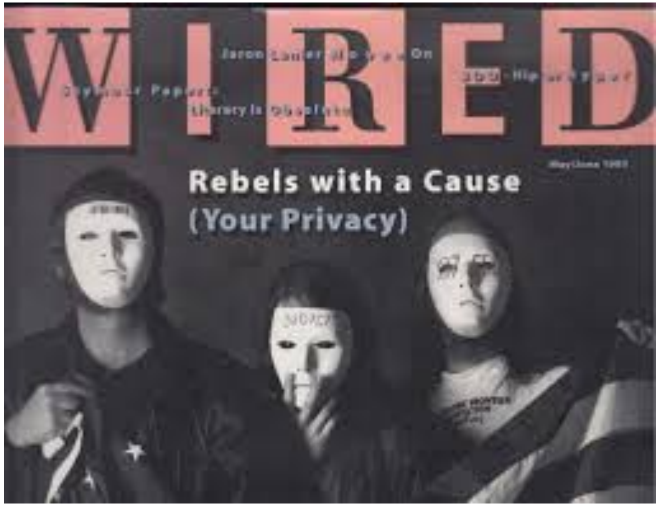
f operations	Time
	3.9 hours
	104 days
	74 years
	3.8×10^9 year
	4.9×10^{15} yea
	4.2×10^{25} yea

For our scenarios we suppose that A and B (also known as Alice and Bob) are two users of a public-key cryptosystem. We will distinguish their encryption and decryption procedures with subscripts: E_A, D_A, E_B, D_B.

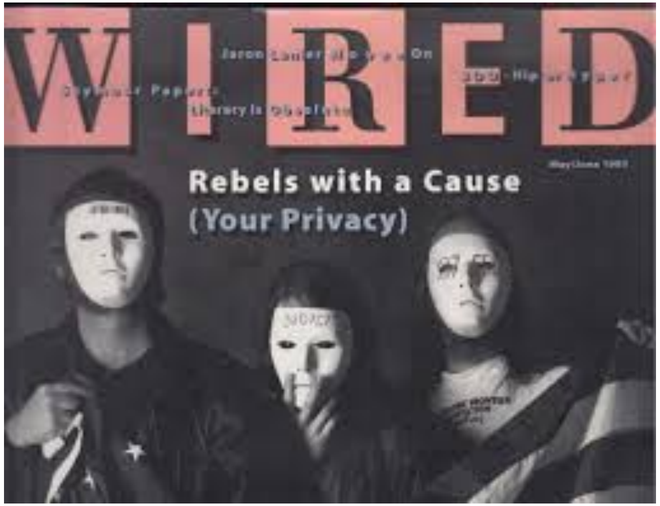
Meet Alice,

and Bob.

For our scenarios we suppose that A and B (also kno
two users of a public-key cryptosystem. We will disting
decryption procedures with subscripts: E_A, D_A, E_B, D_B.



, and .



, and .

```
From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST
```

Cypherpunks of the World,

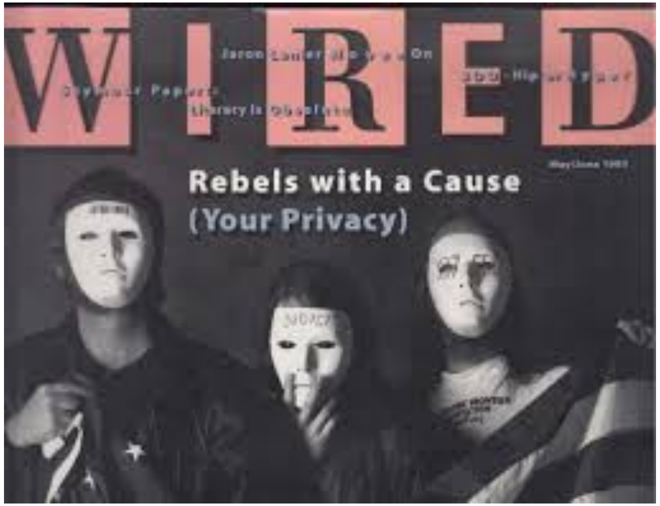
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May



, and .

The technology for this revolution — and it surely will be both a social and economic revolution — has existed in theory for the past decade. The methods are based upon **public-key encryption, zero-knowledge interactive proof systems,** and various software protocols for **interaction, authentication,** and **verification.**

```
From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST
```

Cypherpunks of the World,

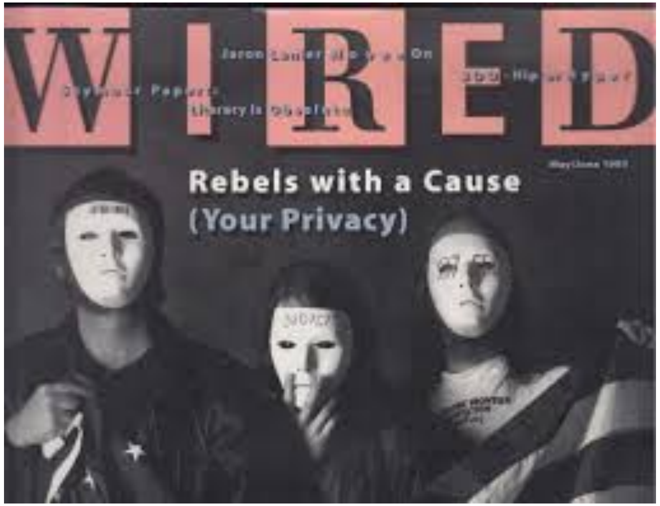
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May



, and .

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts **without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable**, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today.

The technology for this revolution — and it surely will be both a social and economic revolution — has existed in theory for the past decade. The methods are based upon **public-key encryption, zero-knowledge interactive proof systems**, and various software protocols for **interaction, authentication, and verification.**

```
From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST
```

Cypherpunks of the World,

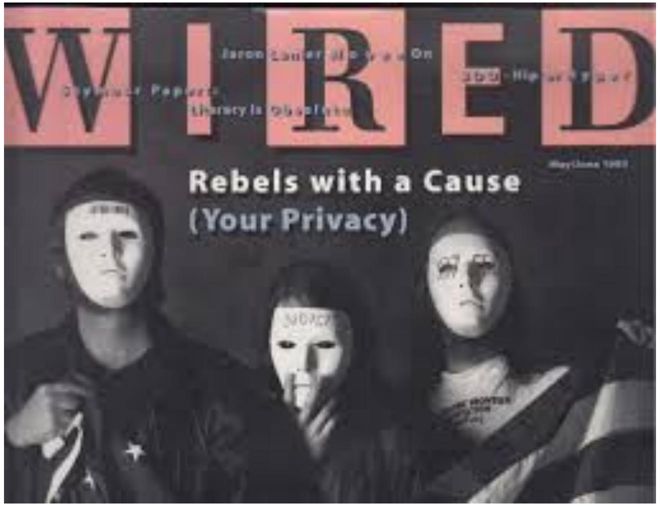
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May



Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts **without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable**, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any

ir

The technology for this revolution — and it surely will be both a social and economic revolution — has existed in theory for the past decade. The methods are based upon **public-key encryption, zero-knowledge interactive proof systems,** and various software protocols for **interaction, authentication, and verification.**

These developments will alter completely the nature of government regulation, the **ability to tax and control economic interactions,** the **ability to keep information secret,** and will even alter the nature of trust and reputation.

, and .

```
From: tcmay@netcom.com (Timothy C. May)
Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST
```

Cypherpunks of the World,

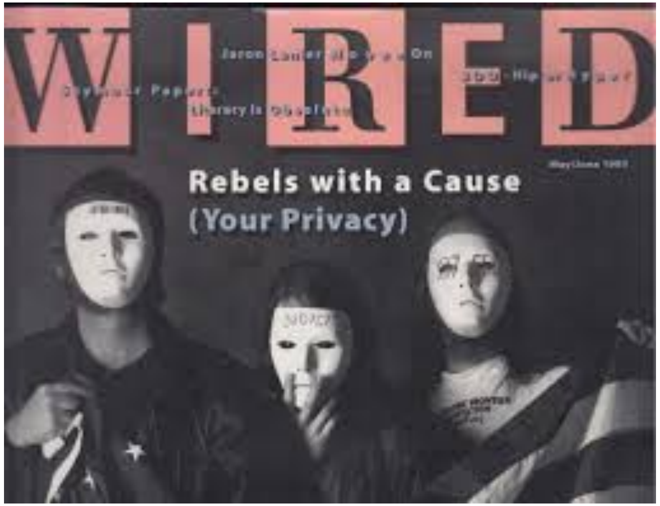
Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May



, and .

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts **without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable**, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any

ir

The technology for this revolution — and it surely will be both a social and economic revolution — has existed in theory for the past decade. The methods are based upon **public-key encryption, zero-knowledge interactive proof systems,** and various software protocols for **interaction, authentication, and verification.**

These developments will alter completely the nature of government regulation, the **ability to tax and control economic interactions**, the **ability to keep information secret**, and will even alter the nature of trust and reputation.

An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will **not halt the spread of crypto anarchy.**

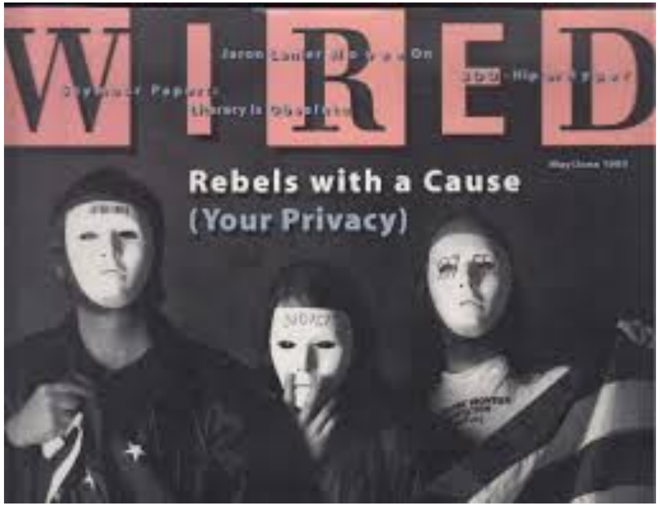
ay in Silicon Valley requested that more of the material passed out in
he Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May



, and .

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts **without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable**, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any

ir

These developments will alter completely the nature of government regulation, the **ability to tax and control economic interactions**, the **ability to keep information secret**, and will even alter the nature of trust and reputation.

The technology for this revolution — and it surely will be both a social and economic revolution — has existed in theory for the past decade. The methods are based upon **public-key encryption, zero-knowledge interactive proof systems**, and various software protocols for **interaction, authentication, and verification.**

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded.

An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will **not halt the spread of crypto anarchy.**

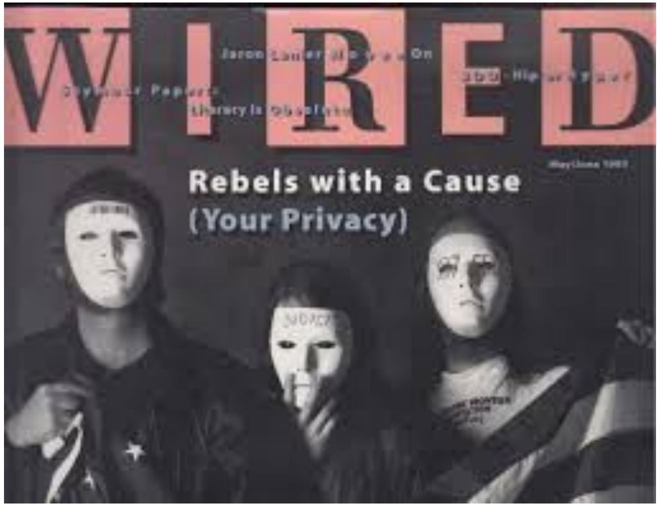
ay in Silicon Valley requested that more of the material passed out in
he Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed t some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talk Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May



Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts **without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable**, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any

ir

The technology for this revolution — and it surely will be both a social and economic revolution — has existed in theory for the past decade. The methods are based upon **public-key encryption, zero-knowledge interactive proof systems,** and various software protocols for **interaction, authentication, and verification.**

, and .

An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will **not halt the spread of crypto anarchy.**

These developments will alter completely the nature of government regulation, the **ability to tax and control economic interactions,** the **ability to keep information secret,** and will even alter the nature of trust and reputation.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded.

ay in Silicon Valley requested that more of the material passed out in
he Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to
some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talk
Hackers on this in

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods **fundamentally alter the nature of corporations and of government interference in economic transactions.**

There are a few thi hope the
Crypto Glossary I j

(This should explai

--Tim May

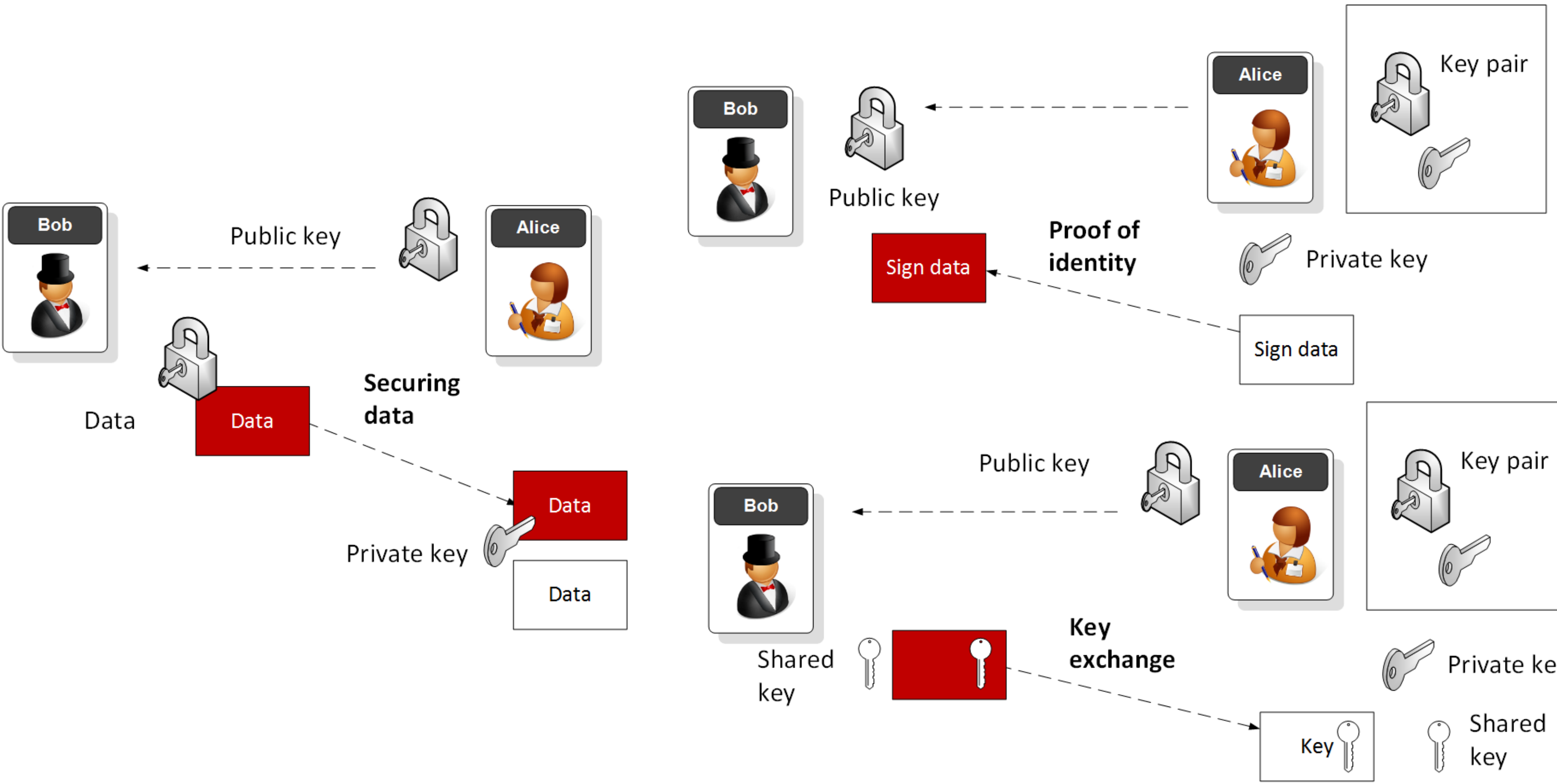
Chapter 4: Public Key

Basics
RSA (Factorizing Primes)
Elliptic Curve (Elliptic Curves)
ElGamal (Discrete Logs)

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption

Public Key Methods



Public Key Methods

- **Integer Factorization**. Using prime numbers. Example: RSA. Digital Certs/SSL.
- **Discrete Logarithms**. $Y = G^x \bmod P$. Example: ElGamal.
- **Elliptic Curve Relationships**. Example: Elliptic Curve. Smart Cards, IoT, Tor, Bitcoin.

Public Key Methods

- **Integer Factorization**. Using prime numbers. Example: RSA. Digital Certs/SSL.
- **Discrete Logarithms**. $Y = G^x \bmod P$. Example: ElGamal.
- **Elliptic Curve Relationships**. Example: Elliptic Curve. Smart Cards, IoT, Tor, Bitcoin.

Public Key Methods

- **Integer Factorization**. Using prime numbers. Example: RSA. Digital Certs/SSL
- **Di**
  El
- **El**
  Cu

security level	volume of water to bring to a boil	symmetric key	cryptographic hash	RSA modulus
teaspoon security	0.0025 liter	35	70	242
shower security	80 liter	50	100	453
pool security	2 500 000 liter	65	130	745
rain security	0.082 km^3	80	160	1130
lake security	89 km^3	90	180	1440
sea security	3 750 000 km^3	105	210	1990
global security	1 400 000 000 km^3	114	228	2380
solar security	-	140	280	3730

Chapter 4: Public Key

RSA

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption

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.

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]

RSA

Calc

Example

- 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

RSA

openssl genrsa -out private.pem 1024

$$C = M^e \bmod N$$

$$D = C^d \bmod N$$

$$N = p\ q$$

cat private.pem


```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC3qXK4kCxn3BNk87vJUMwIznU8pTjr10Kma9+Jkj4zEy/fiZtY
xvdmn1rKNq/8fEUDCcRVC8hQBpevqxFiJ3dbA7ZM6VjUAmztOfRfxSezgvkjswVS
F1/cgBM32AB4nx1dkCV/Wgedn3KFIFU+b8LH1ZLoyRMyLnwWmAkT/mBC/QIDAQAB
AoGAE8Yao+Rh44y+SdA0F6irTwdrd+wSBNJYSrKyjo1ARR97uAWIxDYnzNS7Yaoh
qH14sKsMiFuMZZFQI4m3hWnaX7OFjhJvxKjP6+BdXKsnwWxpwec7RS6n9ptA7q1E
aIFfVARyiWjG+q+8Bg8CTaHjGgtYPnfLzJM0Vef6gKg5vgECQQDZSKGxtdbpXwXw
VAC78SyfOOYmWKL1HiZs0nyTOnZmhMSkE4+S38zhDTjITh0cuKTksTFeUku/sRij
4T4Y9iz5AkEA2GMpeeRT3IQntmzQgTc7Rgez73Y/UWFynuErg++9gzI758TO3AoV
lFs4NOUAqhZ5fdwizs6sa0bjYm+BC1mbJQJBAMQVts4QItVSSqK6vDrfh/xctd4v
KUh5oAWe4otfPBCCio7jlDLgwxzp+K9TRxRvUWeMvNe4/uEMKgdiss6GAskCQQCf
MpVZMDriifgNppDgABqDszcWfhCnduI1McQqFT+APn0ETy9Bg8nMlDAN+k061b4c
ctDJBhSj+EtiKFbwWsRhAkAnEPn+6m3djTwJMw82DxK1q2fcIjTR0ng8pyrF2iIR
P7oBP8I4hGix/FOrV8M8virK6iCsslEcZBo39FkEqc0N
-----END RSA PRIVATE KEY-----
```


openssl rsa -in private.pem -text

```
Private-Key: (1024 bit)
modulus:
    00:b7:a9:72:b8:90:2c:67:dc:13:64:f3:bb:c9:50:
    cc:08:ce:75:3c:a5:38:eb:d7:42:a6:6b:df:89:92:
    3e:33:13:2f:df:89:9b:58:c6:f7:66:9f:5a:ca:36:
    af:fc:7c:45:03:09:c4:55:0b:c8:50:06:97:af:ab:
    11:62:27:77:5b:03:b6:4c:e9:58:d4:02:6c:ed:39:
    f4:5f:c5:27:b3:82:f9:23:b3:05:52:17:5f:dc:80:
    13:37:d8:00:78:9f:1d:5d:90:25:7f:5a:07:9d:9f:
    72:85:20:55:3e:6f:c2:c7:d5:92:e8:c9:13:32:2e:
    7c:16:98:09:13:fe:60:42:fd
publicExponent: 65537 (0x10001)
privateExponent:
    13:c6:1a:a3:e4:61:e3:8c:be:49:d0:34:17:a8:ab:
    4f:07:6b:77:ec:12:04:d2:58:4a:b2:b2:8e:8d:40:
    45:1f:7b:b8:05:88:c4:36:27:cc:d4:bb:61:aa:21:
    a8:7d:78:b0:ab:0c:88:5b:8c:65:91:50:23:89:b7:
    85:69:da:5f:b3:85:8e:12:6f:c4:a8:cf:eb:e0:5d:
    5c:ab:27:c1:6c:69:c1:e7:3b:45:2e:a7:f6:9b:40:
    ee:a9:44:68:81:5f:54:04:72:89:68:c6:fa:af:bc:
    06:0f:02:4d:a1:e3:1a:0b:58:3e:77:cb:cc:93:34:
    55:e7:fa:80:a8:39:be:01
prime1:
    00:d9:48:a1:b1:b5:d6:e9:5f:05:f0:54:00:bb:f1:
    2c:9f:38:e6:26:58:a2:f5:1e:26:6c:d2:7c:93:3a:
    76:66:84:c4:a4:13:8f:92:df:cc:e1:0d:38:c8:4e:
    1d:1c:b8:a4:e4:b1:31:5e:52:4b:bf:b1:18:a3:e1:
    3e:18:f6:2c:f9
prime2:
    00:d8:63:29:79:e4:53:dc:84:27:b6:6c:d0:81:37:
    3b:46:07:b3:ef:76:3f:51:61:72:9e:e1:2b:83:ef:
    bd:83:32:3b:e7:c4:ce:dc:0a:15:94:5b:38:34:e5:
    00:aa:16:79:7d:dc:22:ce:ce:ac:6b:46:e3:62:6f:
    81:0b:59:9b:25
```

RSA

openssl genrsa -out private.pem 1024

$$C = M^e \bmod N$$

openssl rsa -in private.pem -text

```
Private-Key: (1024 bit)
modulus:
    00:b7:a9:72:b8:90:2c:67:dc:13:64:f3:bb:c9:50:
    cc:08:ce:75:3c:a5:38:eb:d7:42:a6:6b:df:89:92:
    3e:33:13:2f:df:89:9b:58:c6:f7:66:9f:5a:ca:36:
```

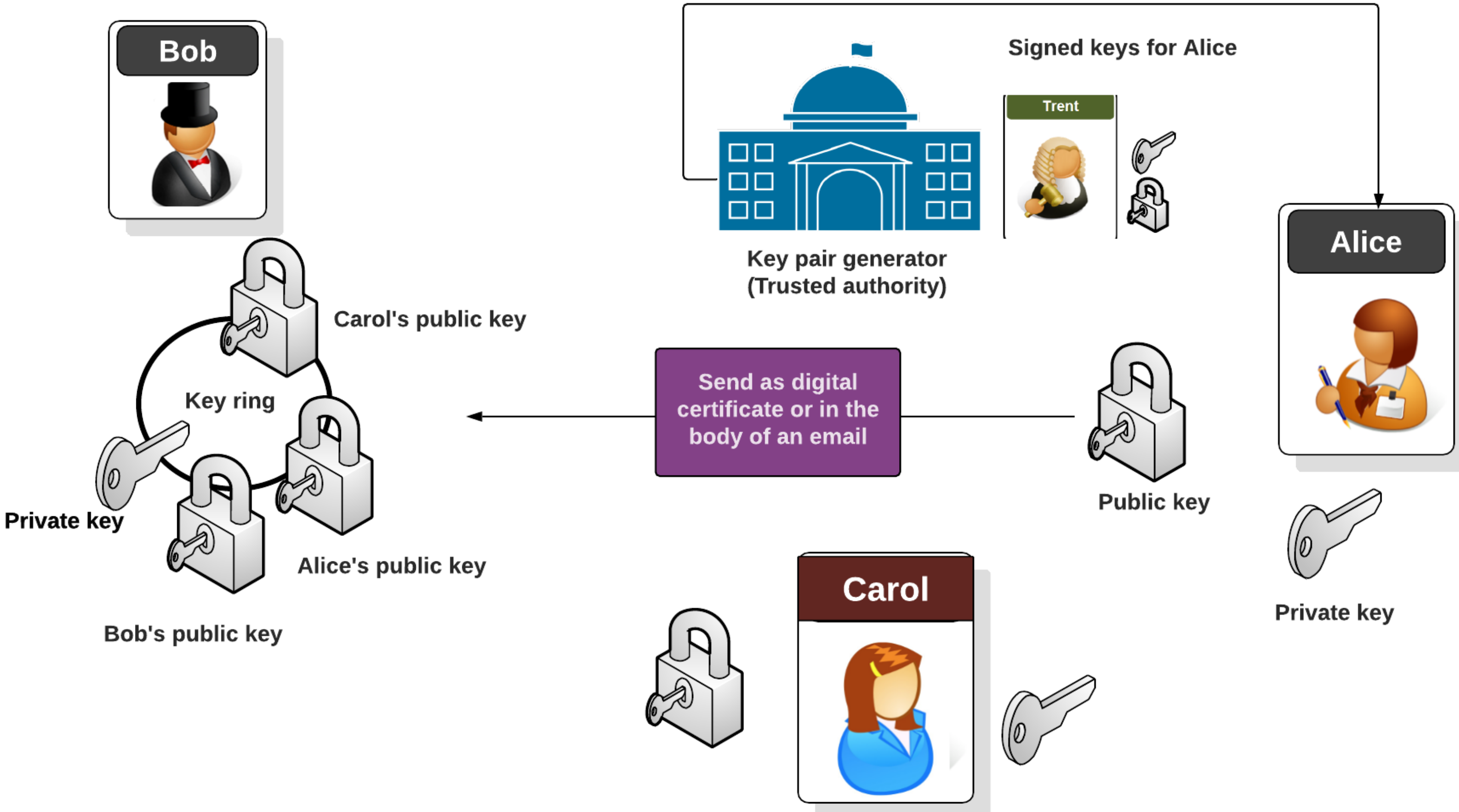
```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQEMA8anVEMIIe/JAQf/cUmIvTbhQQhr70vPY817xRld7NNUrfIqWoz0S7BfpXDi
kvNbw/tIR5yS8gIbm25QFl5kUCukZh3zBq1vZ4pSq35e0ReH4RZQRmDe6Wtn244D
OPJ6WOe4c4y+87shZdJhAwgpLZl5gqZ3YnySoX7kH2CbqDYJUr+4giq/TWGYGb+F
7ztIBwnTZEyijFpWrYhtBVz2DM1HfMDgH3wNWLH0LbE+s7XwqBP/3FHp4Holaqrt
BMU9+MZlM5rqq/AnGXW80/VR8eELJs500qRZmHcI8DO6p8sgNBTeuchadSkKZLgP
iO+l/m2/9nOFg++JSCRpul+JVQU+IngP9pgG13NvktJUAa2/McEaBRYeIr1X4v6g
Syr5jcHBqCR3zyMVO6rg2+r0VK3Z0a9DV4QGOyKewJhPEwPDfLo4SoWZa5n9zwNP
JWm6iiSYz2wLiYd5Pg6Zr/DpGbDF
=5Ost
-----END PGP MESSAGE-----
```

```
MpVZMDriifgNppDgABqDszcWfhCnduI1McQqFT+APn0ETy9Bg8nMlDAN+k061b4c
ctDJBhSj+EtiKFbwWsRhAkAnEPn+6m3djTwJMw82DxK1q2fcIjTR0ng8pyrF2iIR
P7oBP8I4hGix/FOrV8M8virK6iCsslEcZBo39FkEqc0N
-----END RSA PRIVATE KEY-----
```

```
    3e:18:f6:2c:f9
prime2:
    00:d8:63:29:79:e4:53:dc:84:27:b6:6c:d0:81:37:
    3b:46:07:b3:ef:76:3f:51:61:72:9e:e1:2b:83:ef:
    bd:83:32:3b:e7:c4:ce:dc:0a:15:94:5b:38:34:e5:
    00:aa:16:79:7d:dc:22:ce:ce:ac:6b:46:e3:62:6f:
    81:0b:59:9b:25
```

Key ring


Bob
Carol's public key
Key ring
Private key
Alice's public key
Bob's public key
Signed keys for Alice
Trent
Key pair generator
(Trusted authority)
Alice
Send as digital certificate or in the body of an email
Public key
Private key
Carol

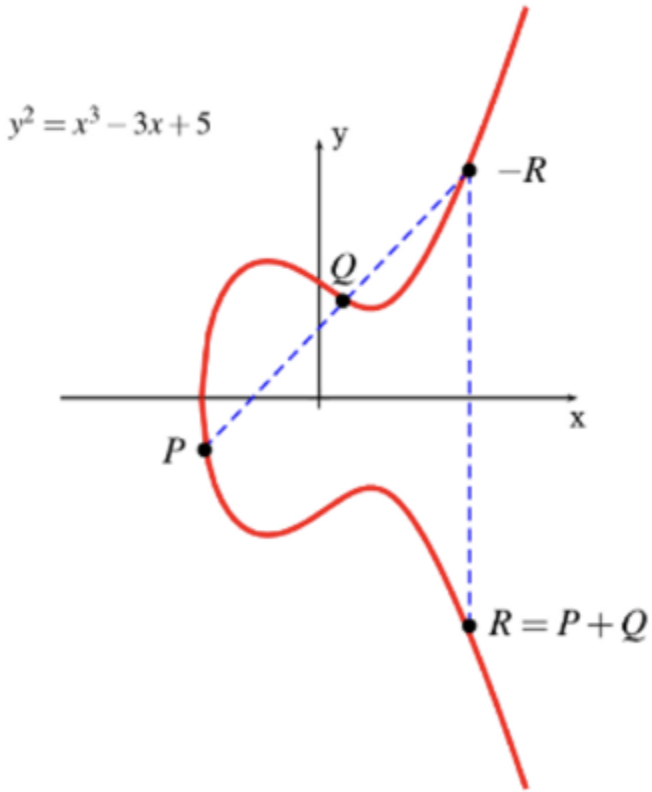
Chapter 4: Public Key

Elliptic Curve

Prof Bill Buchanan OBE

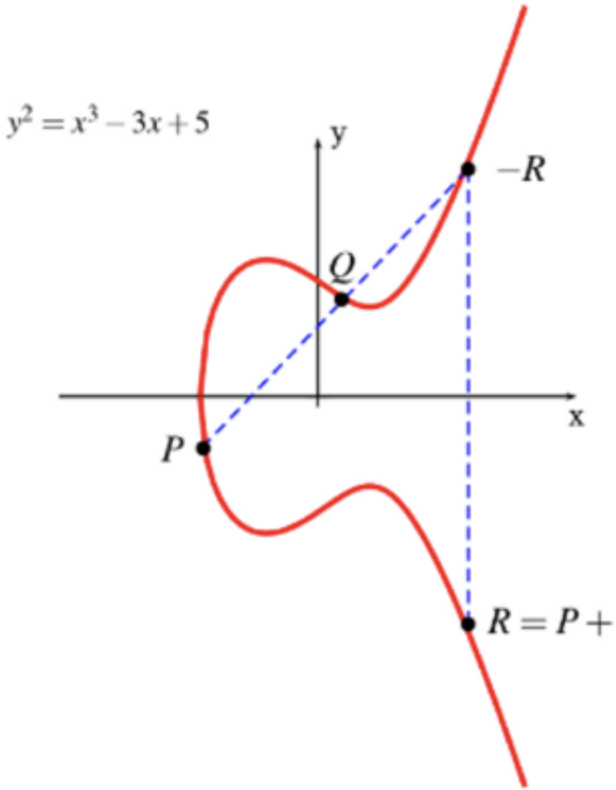
http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption

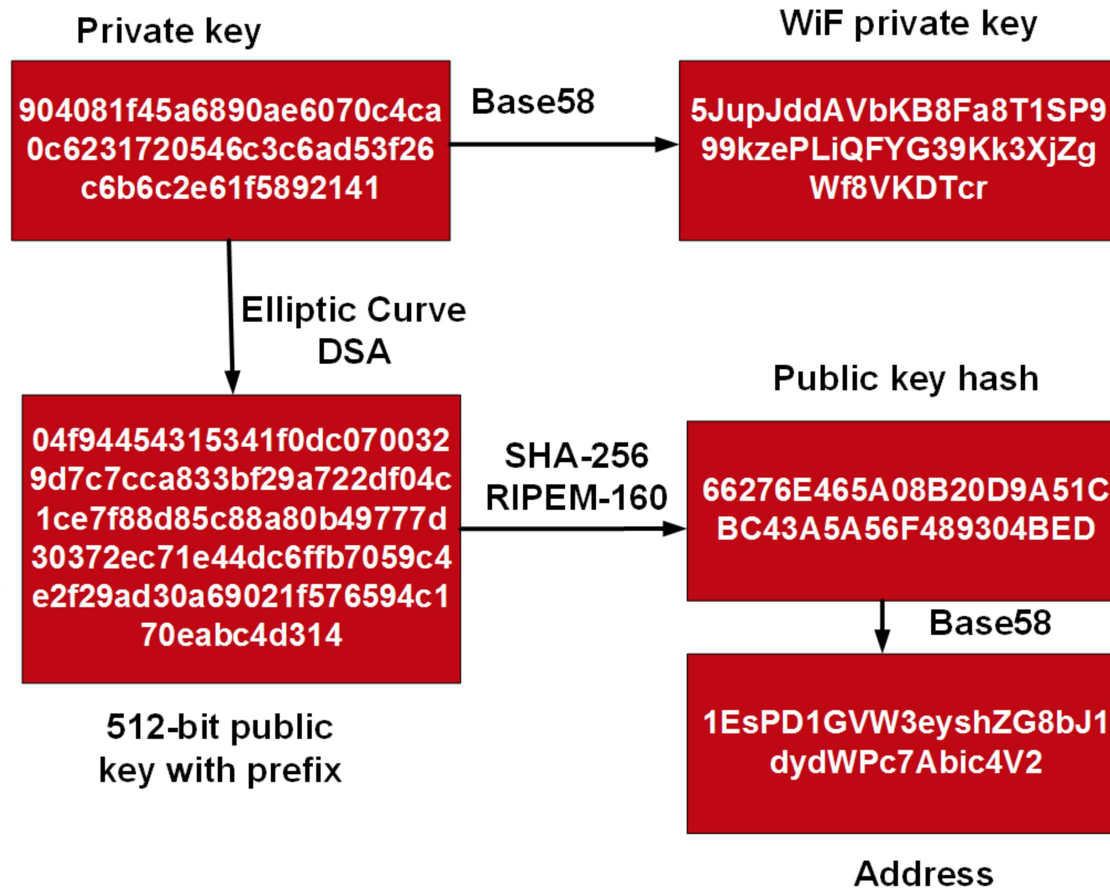
Elliptic Curve (EC)



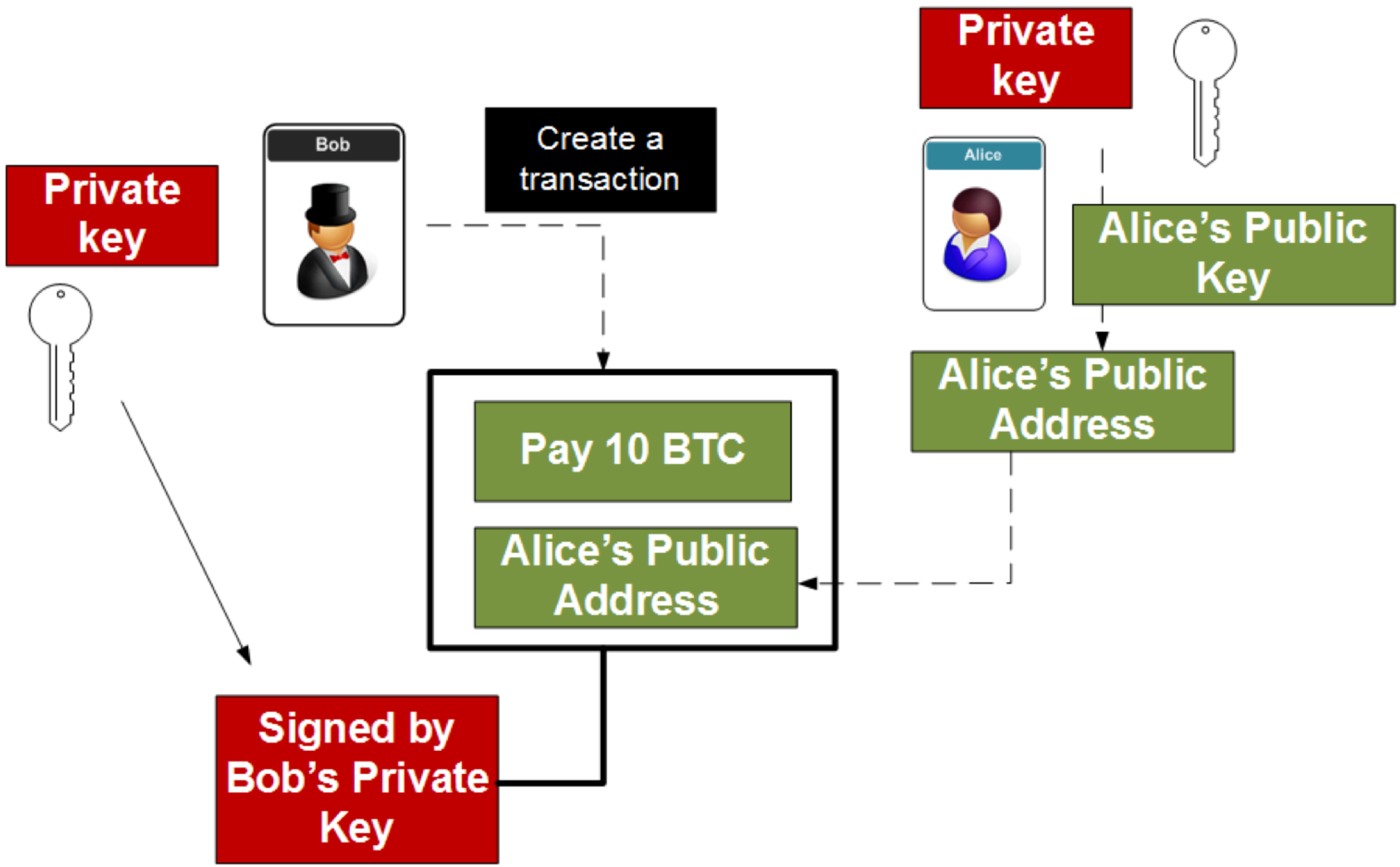
- Pick a point on the elliptic curve (G).
- Generate a random number (n) – this will be the private key.
- Public key is P = n x G (mod p), where p is a prime number (eg 256-bit prime for Curve 25519).
- n is a scalar value which multiples with G to give P (public key)
- Bitcoin uses secp256k1 and Tor uses Curve 25519 [here].

Bitcoin Key Generation

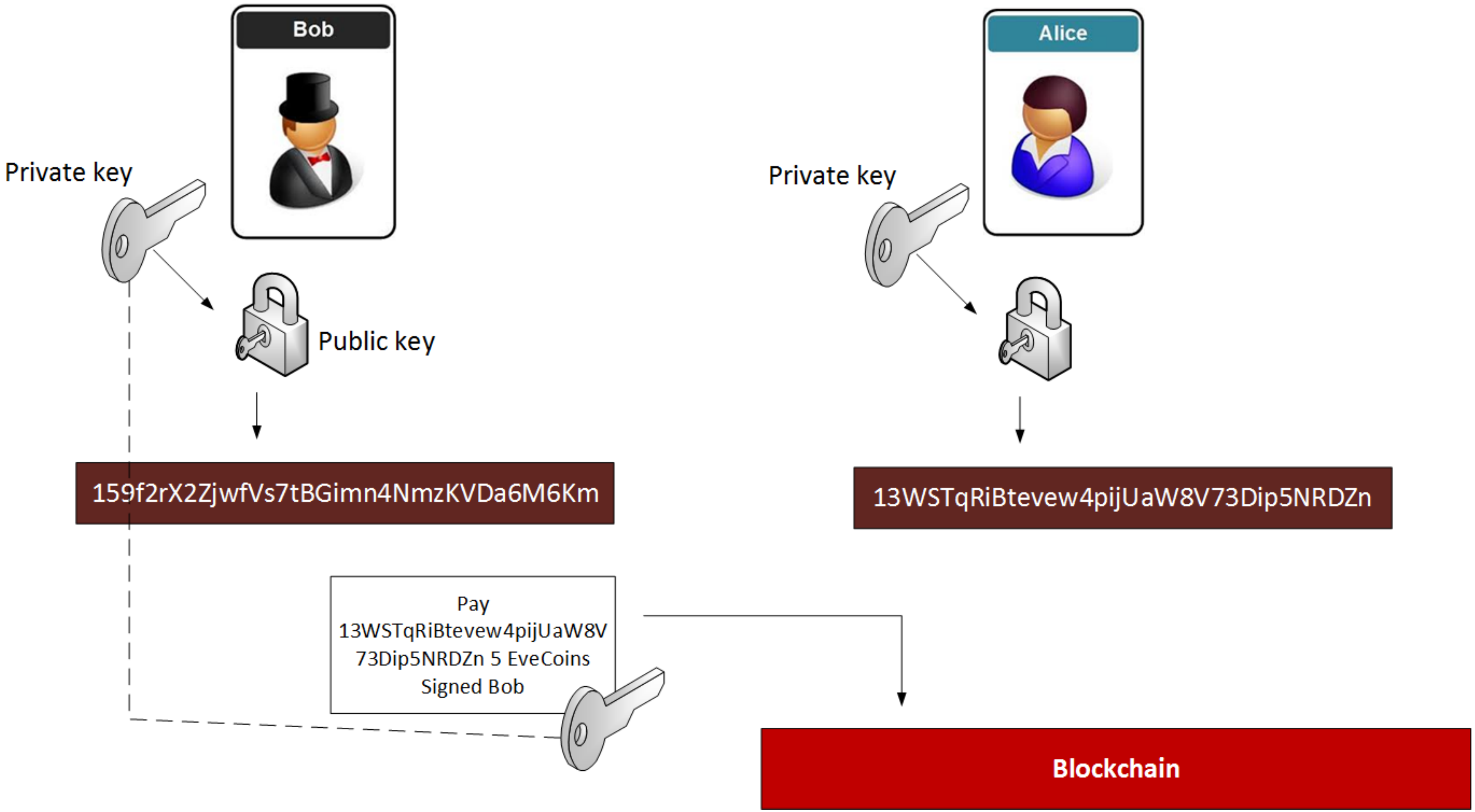




Bitcoin Transaction



Signing


Bob
Private key
Public key
159f2rX2ZjwfVs7tBGimn4NmzKVDa6M6Km
Pay
13WSTqRiBtevew4pijUaW8V
73Dip5NRDZn 5 EveCoins
Signed Bob
Alice
Private key
13WSTqRiBtevew4pijUaW8V73Dip5NRDZn
Blockchain

Example

Elliptic Curve (EC)


```
C \ > openssl ecparam -name secp256k1 -genkey -out priv.pem

C \ > type ec-priv.pem
-----BEGIN EC PARAMETERS-----
BgUrgQQACg==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHQCAQEEIEa56GG2PTUJyIt4FydaMNItYsjNj6ZIbd7jXvDY4ElfoAcGBSuBBAAK
oUQDQgAEJQDn8/vd8oQpA/VE3ch0lM6VAprOTiV9VLp38rwfOog3qUYcTxxX/sxJ
l1M4HncqEopYIKkkovoFFi62Yph6nw==
-----END EC PRIVATE KEY-----
```

Example

Elliptic Curve (EC)

```
C \ > openssl ecparam -name secp256k1 -genkey -out priv.pem

C \ > type ec-priv.pem
-----BEGIN EC PARAMETERS-----
BgUrgQQACg==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHQCAQEEIEa56GG2PTUJyIt4FydaMNItYsjNj6ZIbd7jXvDY4ElfoAcGBSuBBAAK
oUQDQgAEJQDn8/vd8oQpA/VE3ch0lM6VAprOTiV9VLp38rwfOog3qUYcTxxX/sxJ
l1M4HncqEopYIKkkovoFFi62Yph6nw==
-----END EC PRIVATE KEY-----
```

Example

Elliptic Curve (EC)

```
C \ > openssl ecparam -name secp256k1 -genkey -out priv.pem

C \ >
-----B
BgUr
-----E
-----B
MHC
oUQ
l1M4
-----E
```

```
C \> openssl ec -in priv.pem -text -noout
read EC key
Private-Key  (256 bit)
priv
    46 b9 e8 61 b6 3d 35 09 c8 8b 78 17 27 5a 30
    d2 2d 62 c8 cd 8f a6 48 6d de e3 5e f0 d8 e0
    49 5f
pub
    04 25 00 e7 f3 fb dd f2 84 29 03 f5 44 dd c8
    74 94 ce 95 02 9a ce 4e 25 7d 54 ba 77 f2 bc
    1f 3a 88 37 a9 46 1c 4f 1c 57 fe cc 49 97 53
    38 1e 77 2a 12 8a 58 20 a9 24 a2 fa 05 16 2e
    b6 62 98 7a 9f
ASN1 OID  secp256k1
```

Example

Elliptic Curve (EC)

```
C \ > openssl ecparam -name secp256k1 -genkey -out priv.pem

C \ > type ec-priv.pem
-----BEGIN EC PARAMETERS-----
BgUrgQQACg==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHQCAQEEIEa56GG2PTUJyIt4FydaMNItYsjNj6ZIbd7jXvDY4ElfoAcGBSuBBAAK
oUQDQgAEJQDn8/vd8oQpA/VE3ch0lM6VAprOTiV9VLp38rwfOog3qUYcTxxX/sxJ
l1M4HncqEopYIKkkovoFFi62Yph6nw==
-----END EC PRIVATE KEY-----
```

Example

Elliptic Curve (EC)

```
C \ > openssl ecparam -name secp256k1 -genkey -out priv.pem

C \ >
-----B
BgUr
-----E
-----B
MHC
oUQ
l1M4
-----E
```

```
C \> openssl ec -in priv.pem -text -noout
read EC key
Private-Key  (256 bit)
priv
    46 b9 e8 61 b6 3d 35 09 c8 8b 78 17 27 5a 30
    d2 2d 62 c8 cd 8f a6 48 6d de e3 5e f0 d8 e0
    49 5f
pub
    04 25 00 e7 f3 fb dd f2 84 29 03 f5 44 dd c8
    74 94 ce 95 02 9a ce 4e 25 7d 54 ba 77 f2 bc
    1f 3a 88 37 a9 46 1c 4f 1c 57 fe cc 49 97 53
    38 1e 77 2a 12 8a 58 20 a9 24 a2 fa 05 16 2e
    b6 62 98 7a 9f
ASN1 OID  secp256k1
```

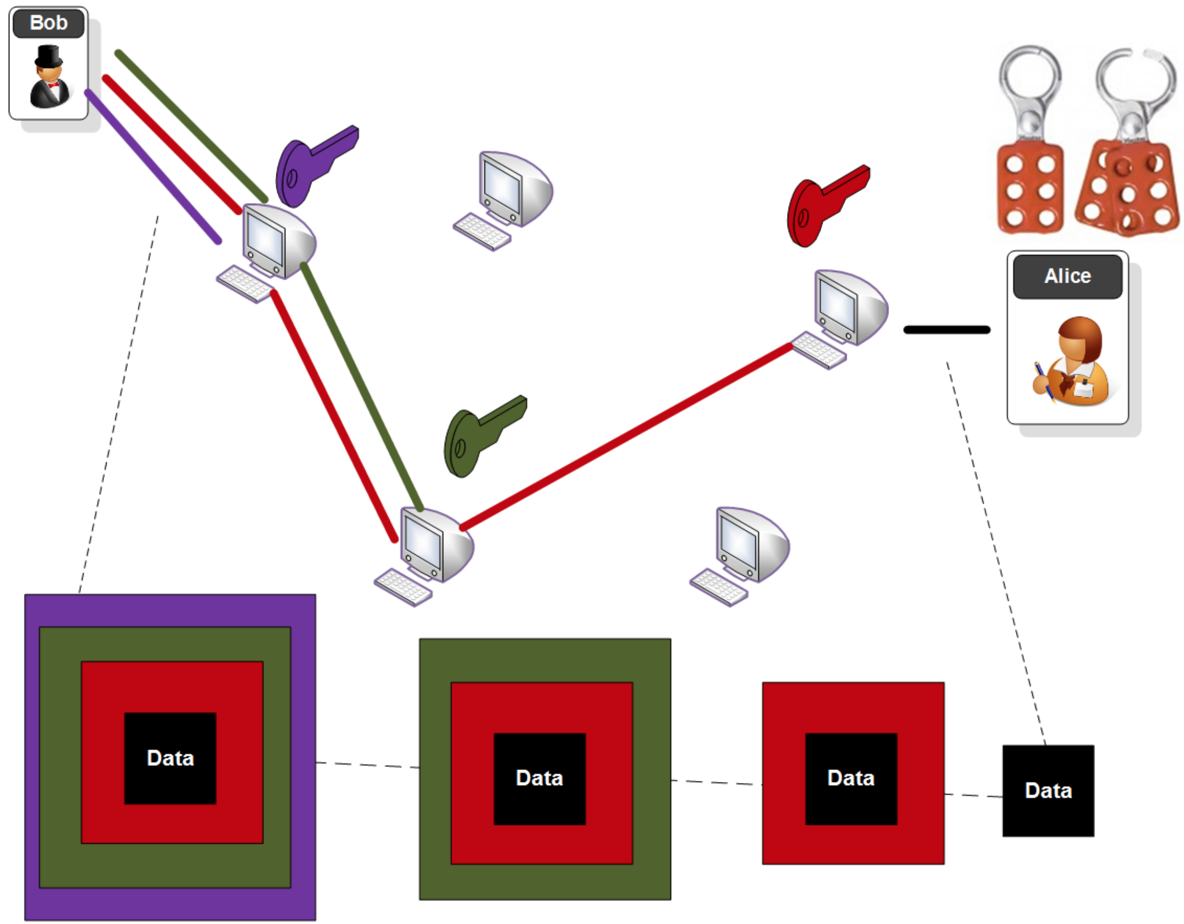
[Example]()

```
C \ > open
C \ >
-----B
BgUr
-----E
-----B
MHC
oUQ
l1M4
-----E
```

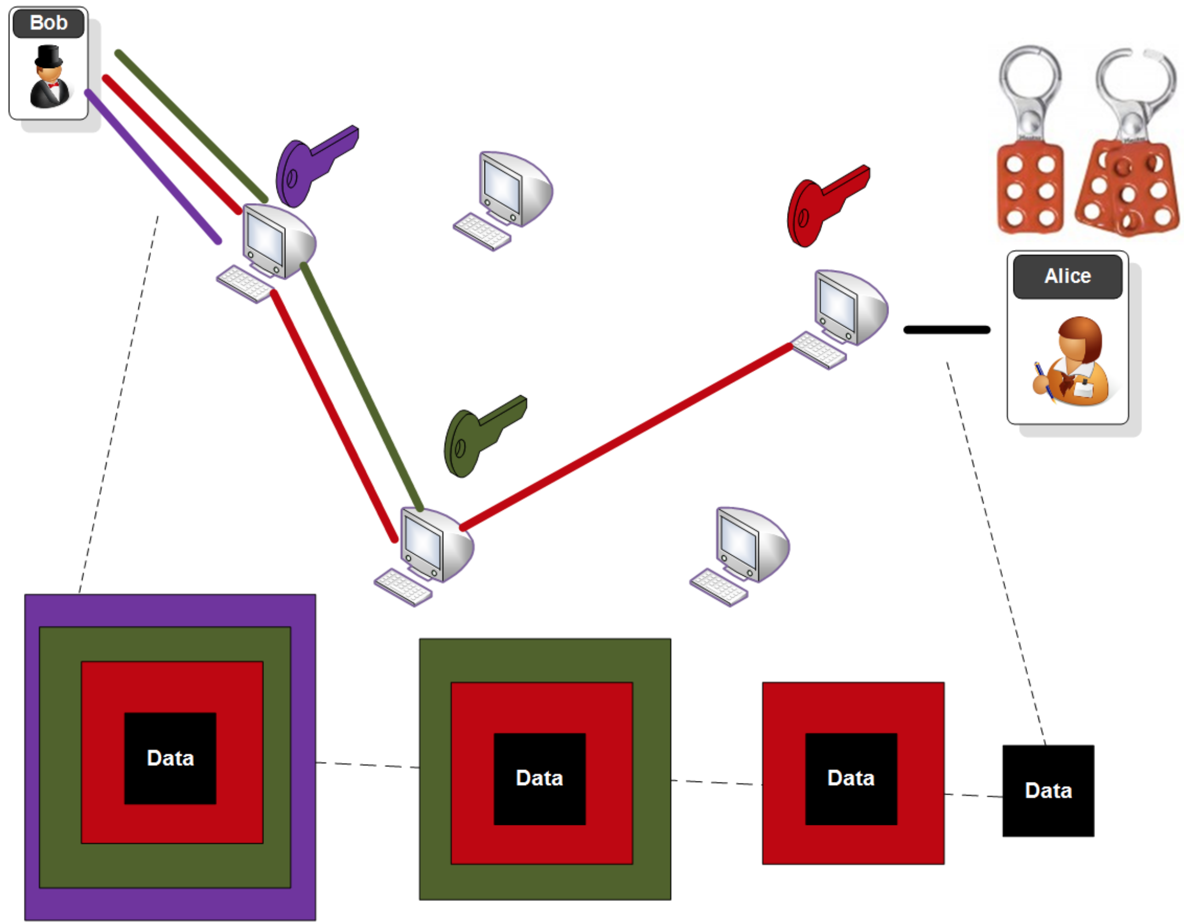
```
C \>
read
Priva
priv
   46
   d2
   49
pub
   04
   74
   1f
   38
   b6
ASN1
```

```
C:> openssl ecparam -in priv.pem -text -param_enc explicit -noout
Field Type: prime-field
Prime:
    00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:fe:ff:
    ff:fc:2f
A:    0
B:    7 (0x7)
Generator (uncompressed):
    04:79:be:66:7e:f9:dc:bb:ac:55:a0:62:95:ce:87:
    0b:07:02:9b:fc:db:2d:ce:28:d9:59:f2:81:5b:16:
    f8:17:98:48:3a:da:77:26:a3:c4:65:5d:a4:fb:fc:
    0e:11:08:a8:fd:17:b4:48:a6:85:54:19:9c:47:d0:
    8f:fb:10:d4:b8
Order:
    00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:fe:ba:ae:dc:e6:af:48:a0:3b:bf:d2:5e:8c:d0:
    36:41:41
Cofactor:  1 (0x1)
```

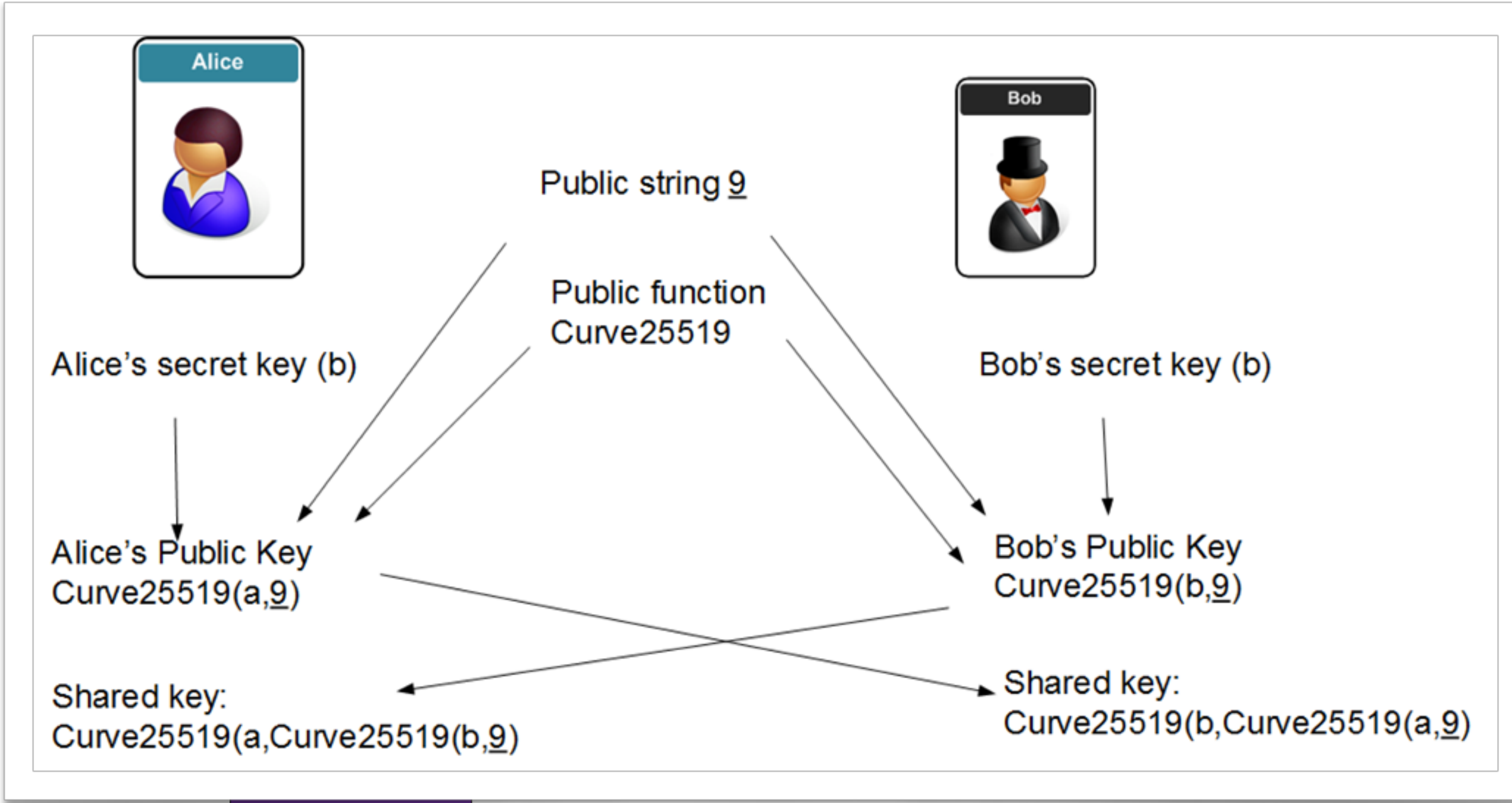
Elliptic Curve Diffie Hellman (ECDH)



Elliptic Curve Diffie Hellman (ECDH)



Elliptic Curve Diffie Hellman (ECDH)



Chapter 4: Public Key

ElGamal

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption

ElGamal

- $Y = G^x \bmod p$
- G is picked from cyclic group (Explained in Key Handshaking section). Here.
- p is a prime number.
- Example here.

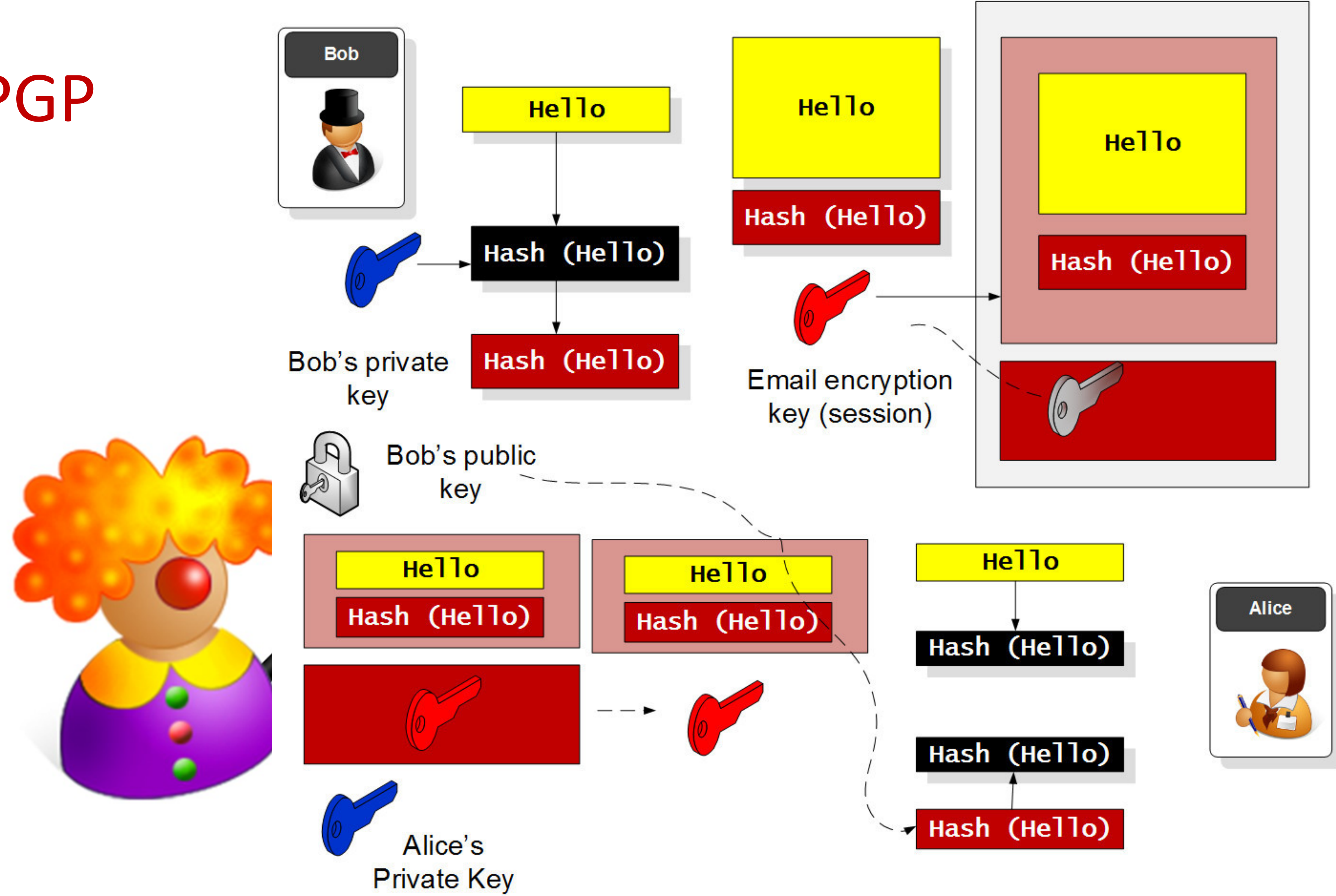
Chapter 4: Public Key

PGP

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption

PGP



Bob
Hello
Hash (Hello)
Hash (Hello)
Bob's private key
Hello
Hash (Hello)
Email encryption key (session)
Hello
Hash (Hello)
Bob's public key
Hello
Hash (Hello)
Hello
Hash (Hello)
Alice's Private Key
Hello
Hash (Hello)
Hash (Hello)
Hash (Hello)
Alice

Chapter 4: Public Key

Basics
RSA
Elliptic Curve
ElGamal

Prof Bill Buchanan OBE

http://asecuritysite.com/crypto04
http://asecuritysite.com/encryption