

# Encryption 101

What It Is, How To Attack It, How To Defend It

Justin Hall  
Director, Security Services



# /usr/bin/whoami

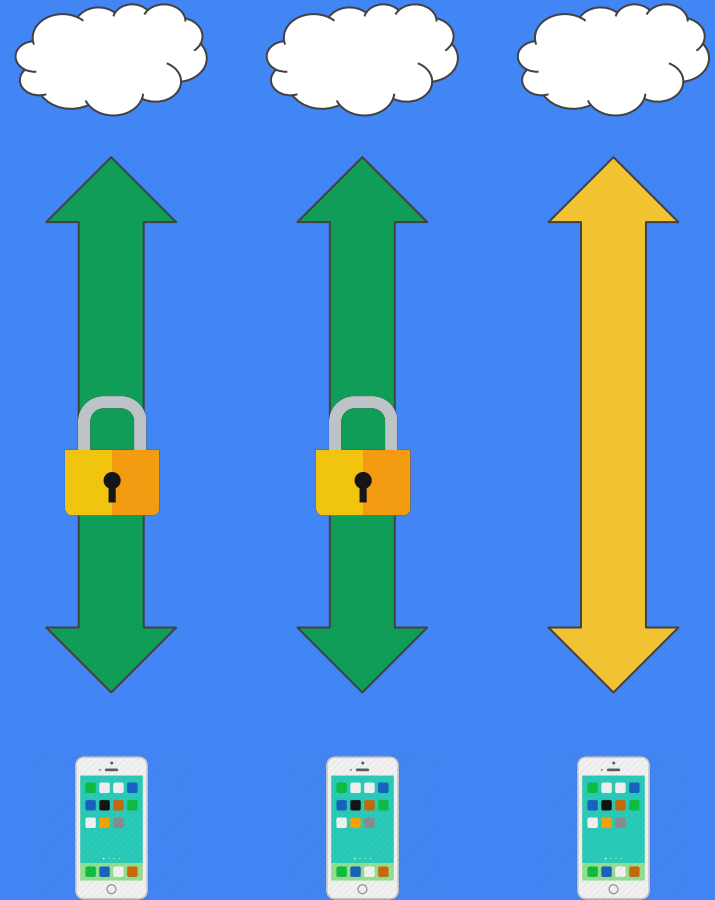
Twelve years with CBTS as security consultant to shops small (5 person) and large (Fortune 5)

GIAC Certified Incident Handler, Forensic Analyst,  
Penetration Tester

BSidesCincinnati cofounder

67% of internet  
traffic will be  
encrypted by  
2016

Source: Sandvine Institute, 2015



Most people  
don't understand  
encryption.

*security practitioners*

Most ~~people~~ ↩  
don't understand  
encryption.

## Why do we encrypt?

Protect sensitive data

Prevent theft

Privacy

name	Email	SSN
XXXXXXi	dXXX@XXXX.com	6XX-XY-XXX0
XXXXXXS	DXXX@XXXX.com	9XX-XY-XXX0
XXXXXXs	pXXX@XXXX.com	7XX-XY-XXX2
XXXXXXI	xXXX@XXXX.com	2XX-XY-XXX6
XXXXXX_	sXXX@XXXX.com	4XX-XY-XXX1
XXXXXXy	sXXX@XXXX.com	0XX-XY-XXX0
XXXXXXy	aXXX@XXXX.com	5XX-XY-XXX2
XXXXXXi	sXXX@XXXX.com	5XX-XY-XXX7
XXXXXXr	dXXX@XXXX.com	3XX-XY-XXX6
XXXXXX_	dXXX@XXXX.com	6XX-XY-XXX6

# Why do we encrypt?

Protect sensitive data

Prevent theft

Privacy

Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
32312	369.903404	192.168.2.5	106.76.209.235	ICMP	70	Destination unreachable (Port unreachable)
32313	369.905837	86.176.100.134	192.168.2.5	TCP	66	64748 > 30149 [SYN] Seq=0 Win=0 Len=0
32314	369.905934	192.168.2.5	86.176.100.134	TCP	54	30149 > 64748 [RST, ACK] Seq=1312111111 Win=0 Len=0
32315	369.907287	49.156.159.35	192.168.2.5	TCP	74	33889 > 30149 [SYN] Seq=0 Win=0 Len=0
32316	369.907357	192.168.2.5	49.156.159.35	TCP	54	30149 > 33889 [RST, ACK] Seq=1312111111 Win=0 Len=0
32317	369.924228	78.60.80.5	192.168.2.5	TCP	66	57058 > 30149 [SYN] Seq=0 Win=0 Len=0
32318	369.924382	192.168.2.5	78.60.80.5	TCP	54	30149 > 57058 [RST, ACK] Seq=1312111111 Win=0 Len=0
32319	369.938434	81.203.200.189	192.168.2.5	TCP	62	52617 > 30149 [SYN] Seq=0 Win=0 Len=0
32320	369.938601	192.168.2.5	81.203.200.189	TCP	54	30149 > 52617 [RST, ACK] Seq=1312111111 Win=0 Len=0
32321	369.939500	46.240.50.22	192.168.2.5	UDP	72	Source port: cap Destination port: 57973
32322	369.939670	192.168.2.5	46.240.50.22	ICMP	70	Destination unreachable (Port unreachable)
32323	369.940294	78.165.164.69	192.168.2.5	TCP	62	51940 > 30149 [SYN] Seq=0 Win=0 Len=0
32324	369.940421	192.168.2.5	78.165.164.69	TCP	54	30149 > 51940 [RST, ACK] Seq=1312111111 Win=0 Len=0
32325	369.950801	186.228.40.136	192.168.2.5	TCP	62	54084 > 30149 [SYN] Seq=0 Win=0 Len=0
32326	369.950955	192.168.2.5	186.228.40.136	TCP	54	30149 > 54084 [RST, ACK] Seq=1312111111 Win=0 Len=0
32327	369.966125	81.203.200.189	192.168.2.5	UDP	72	Source port: 20319 Destination port: 57973
32328	369.966277	192.168.2.5	81.203.200.189	ICMP	70	Destination unreachable (Port unreachable)
32329	369.975934	90.14.19.81	192.168.2.5	UDP	72	Source port: 57973 Destination port: 57973
32330	369.976107	192.168.2.5	90.14.19.81	ICMP	70	Destination unreachable (Port unreachable)
32331	369.981771	89.195.2.222	192.168.2.5	TCP	66	64797 > 30149 [SYN] Seq=0 Win=0 Len=0
32332	369.981918	192.168.2.5	89.195.2.222	TCP	54	30149 > 64797 [RST, ACK] Seq=1312111111 Win=0 Len=0
32333	369.999197	41.96.92.136	192.168.2.5	UDP	109	Source port: 49000 Destination port: 57973

▶ Ethernet II, Src: Apple [REDACTED], Dst: BelkinIn [REDACTED]

▶ Internet Protocol Version 4, Src: 192.168.2.5 (192.168.2.5), Dst: 121.54.54.36 (121.54.54.36)

▼ Internet Control Message Protocol

- Type: 3 (Destination unreachable)
- Code: 3 (Port unreachable)
- Checksum: 0x680c [correct]

▶ Internet Protocol Version 4, Src: 121.54.54.36 (121.54.54.36), Dst: 192.168.2.5 (192.168.2.5)

▼ User Datagram Protocol, Src Port: 7941 (7941), Dst Port: 30149 (30149)

- Source port: 7941 (7941)
- Destination port: 30149 (30149)
- Length: 38
- Checksum: 0x0000 (none)

0000 00 22 75 e0 f6 e8 10 40 f3 94 86 3e 08 00 45 00 .u....@ ...>..E.  
0010 00 38 b1 a7 00 00 40 01 57 16 c0 a8 02 05 79 36 .8....@. W.....y6  
0020 36 24 03 03 68 0c 00 00 00 00 45 00 00 3a 48 dc 6\$.h.... ..E..H.  
0030 00 00 67 11 98 cf 79 36 36 24 c0 a8 02 05 1f 05 ..g...y6 6\$.....  
0040 75 c5 00 26 00 00 u...&..

en1: <live capture in progress> Packets: 138102 Displayed: 138102 Marked: 0

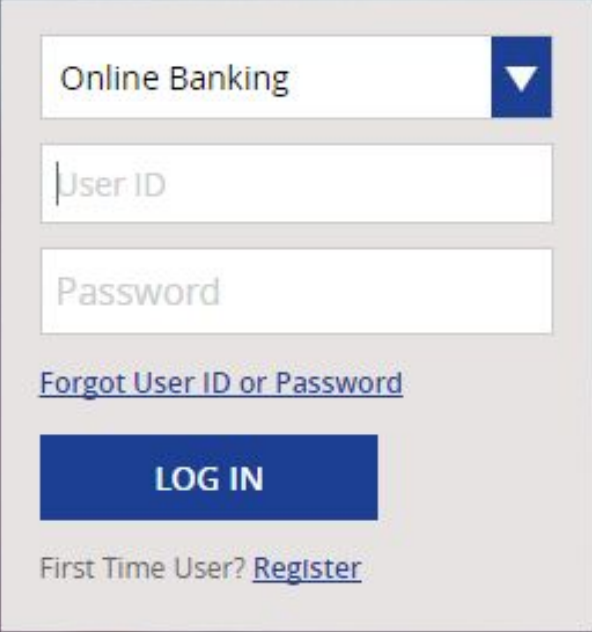
# Why do we encrypt?

Protect sensitive data

Prevent theft

Privacy

## log in



Online Banking ▼

User ID

Password

[Forgot User ID or Password](#)

**LOG IN**

First Time User? [Register](#)

## Existing User

To access your accounts, enter your Social Security number and your password.

## First Time User

### User ID:

Use your Fifth Third debit card number.

Password to change User ID.

### Password:

Use your Card PIN (Personal Identification Number) the first time using your card.





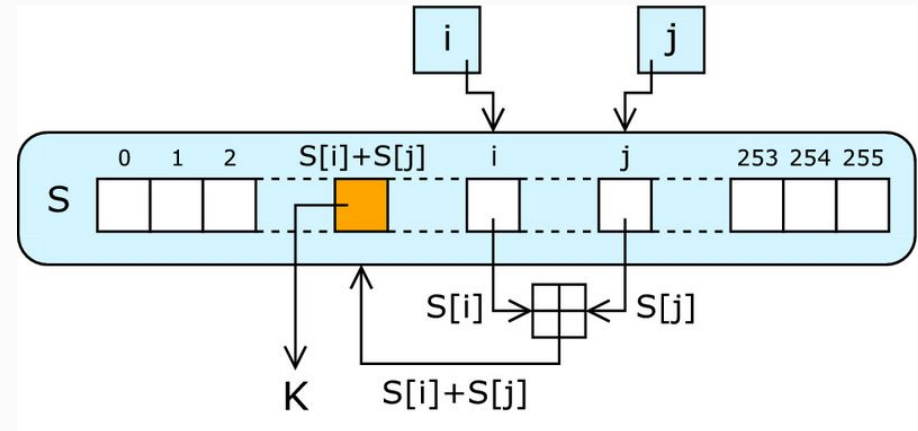
Data At Rest

# Data In Motion



# Ciphers

The algorithm that describes how to encrypt/decrypt data



# Example

ROT13

Frr gur onyy, uvg gur onyy.

## Example

ROT13

See the ball, hit the ball.



ROT13



Frr gur onyy, uvg gur onyy.

# Example

Base64

See the ball, hit the ball.



BASE64

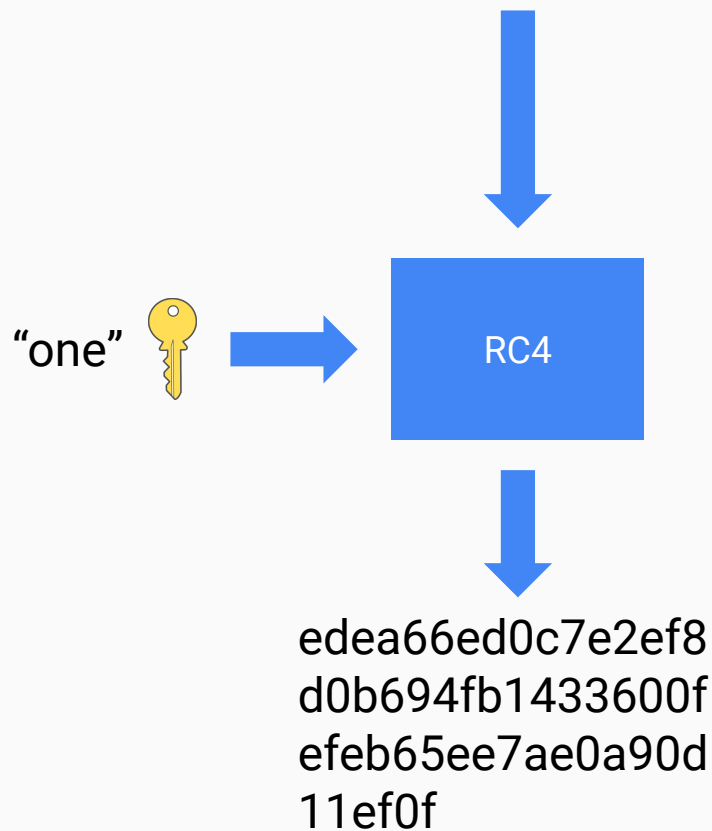


U2VIIHRoZSBiYWxsLCBoaXQgdGhlIGJhbGwu

See the ball, hit the ball.

## Example

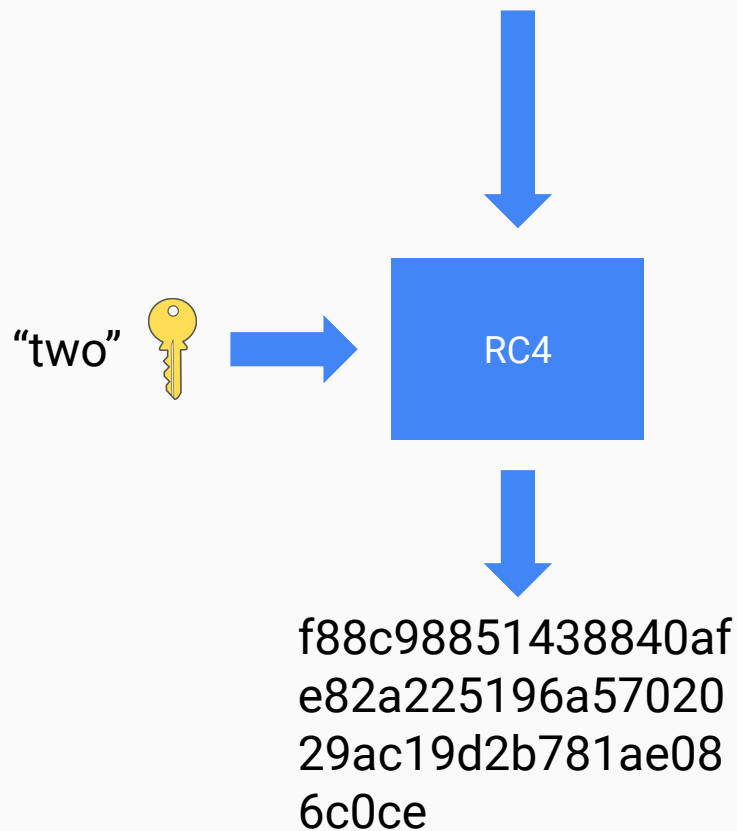
RC4



See the ball, hit the ball.

## Example

RC4





# Key

Variable that  
determines the output  
of the algorithm

```
1 -----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQEARxT6WCxFfda/3xLAKj3gUwtuzvWP05a0w2R8KdRDeRNBLe9
3 AHxBNnTpnCOoGD8s6xx/1LlQOwYKCqoyXUWYREs9GMWqvuhQKUJjxmQCBKTAgrFS
4 A6WUTc0bVyeBgdNtURynZwT29nOPyl8WCqrfBnsjmtWK37eOvb0wmrhotr0hpseX
5 fUcC/MmR3Ewr10He6HBK1AaYltXxEg5Ilw7xTimWlQQZ8NWxZ0vBCSIYoOx10wed
6 /srxNe1gu08nCKxhzX0xT3dZqMi4/7l0xDi0pAiUYOiqxPjujMM3l3HXBrz3uXM0
7 MQH687uAkBB/qRXKzHlI3v2wDh24sQpl/saA3wIDAQABAoIBADbVhH2xPw5LLGpD
8 qBVSrae0g+6jL3k30MME/HHpPXx00ExXYt81Tul3+f7rtBxMLMtiLNeWkcx/AEd
9 Dorxmd+BpM/WUERb44cYeMEQXyVvJ6+kxAKWqkHHJHuIH+01H6pt6/m+SV0Scs6
10 fl+25gRUmnEKgeTQyw6Xatp5+KmKC1MPoXsMmou58q+Zxv+S82QHbxAQlUyjbApT
11 3dqBE9h01I/ar8fY3KV9FIhDribj5mZMUJ4aRLqp0R33nkrjQAkaRLjpbnpIuzZs
12 XMQdX5xU+6L02i4J2UpieVkvVvUjGkyepa7xdyNJ3qUI2VOWW6FxoMio8Jlrdea
13 ljEyKcECgYEA4icfHVKr09kEHSByAEfYrWRkM9ISpxL5wy4KA5827cmLWD+UYlyI
14 YkSPQrF6STA55Th9RJ7IaMgZ3JyuvhGDZmWrJPPw0QRmkYrd2b7KlN8QAcxQYqs2
15 4TDiPRzPlORJbnQaP5+TElHC3cLkZ1z3WCqcZ0CAWp0gSrGo03eIE6ECgYEAxjBb
16 oHYW2t7qm1Exe7rKjhAN5XJ+k18Rw/n+msZkDTq4205uA051xi94Efa3QjfovgBe
17 yIzwBpPiwqW+2jXXMA95K7Ycr9CIuwryGCOTHwmGgtc+BztlcGae47WnLgfbKQLI
18 KiVFyqgx4oI4ZQ+DQSmZfJ4CUWBSNE7tp1JORH8CgYAt5gy9kcrH2zKniq84eVxz
```

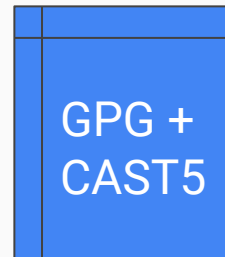
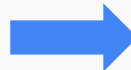
# Symmetric key encryption

**For use by:** individual protecting data from unauthorized access by anyone without key

**One key** locks and unlocks the data

**You must** protect the key

"A very strong passphrase! Really!"



secret.docx



secret.docx.gpg

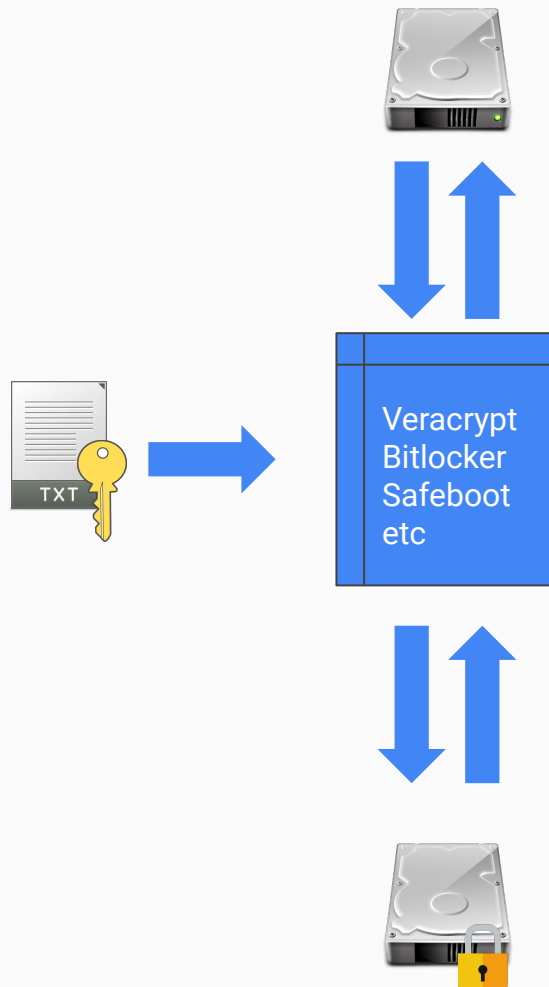


# Symmetric key encryption

**One key** locks and unlocks the data

**You must** protect the key

Keys can be **passwords** or **passphrases**, **key files**, etc



# Asymmetric key encryption

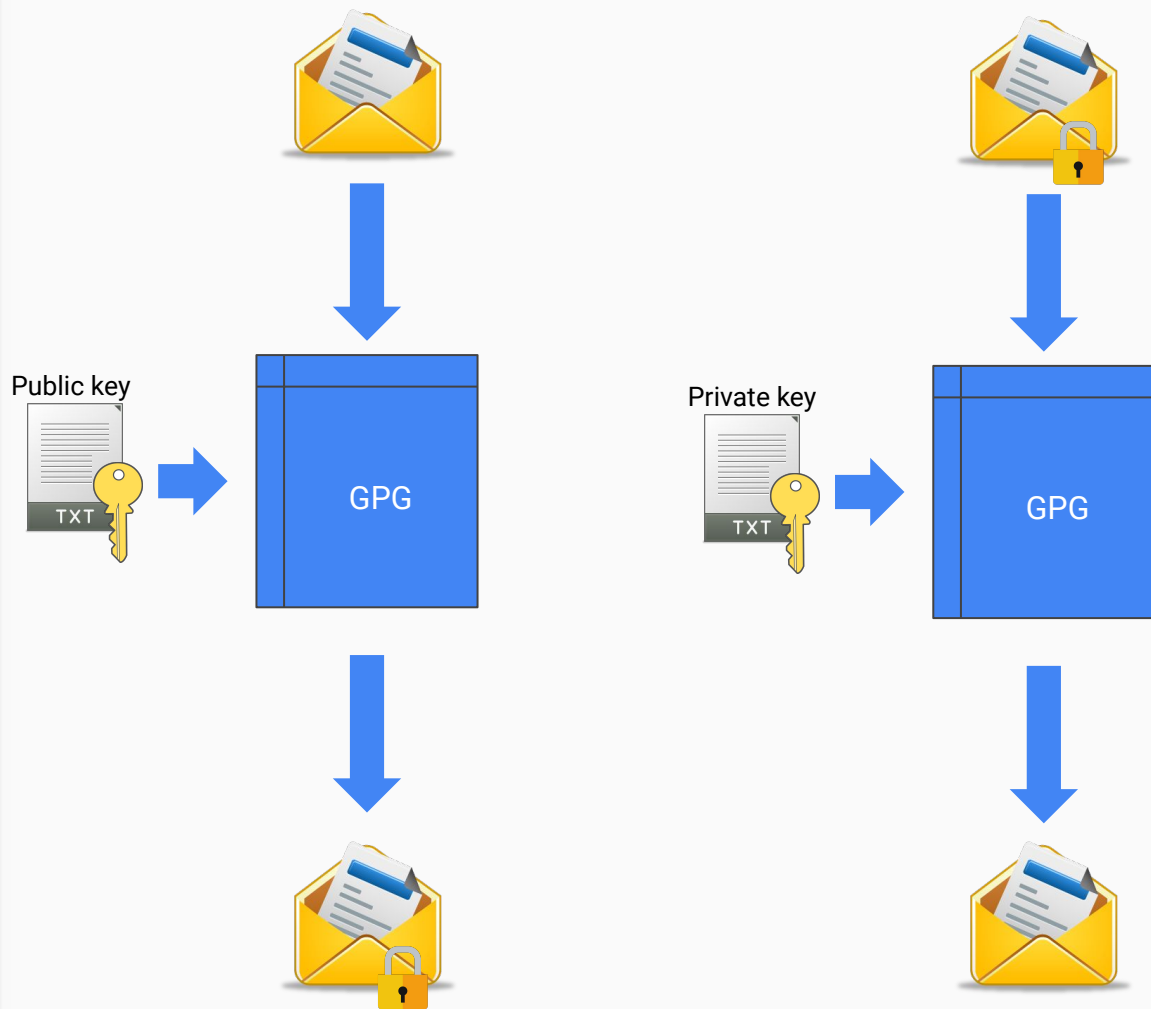
**For use by:** two parties who want communication to remain secret from a third party

**One key** locks the data

A corresponding **second key** unlocks the data

One key is typically **public**

One key is typically **private**



# Public key

Anyone can have it

Anyone can encrypt  
data that's meant for  
me

# Private key

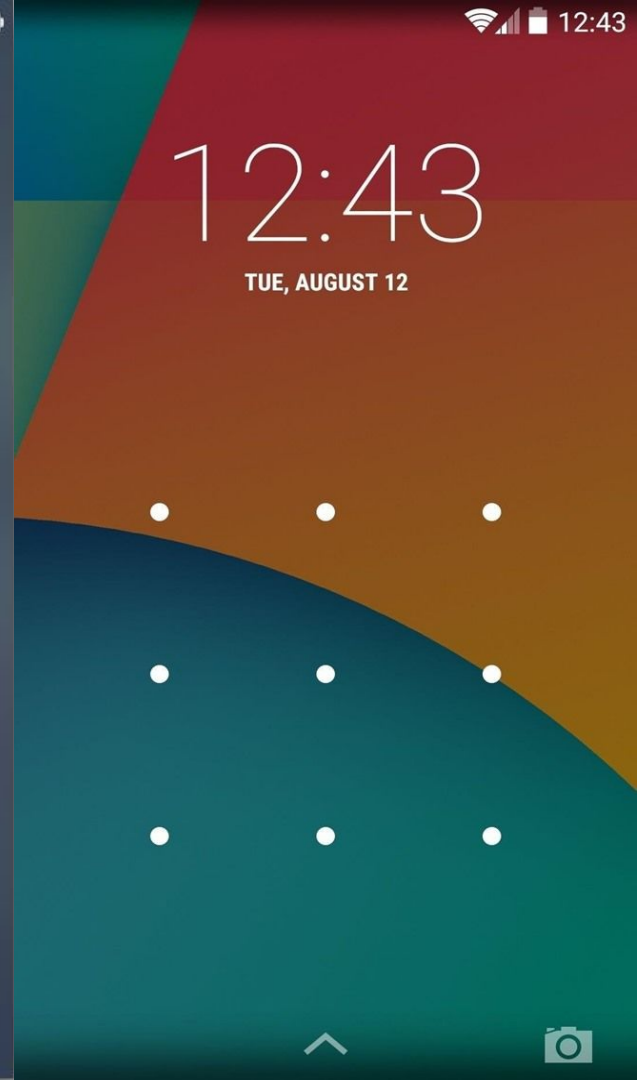
Only I have it

Only I can decrypt  
data that's meant for  
me

# Defeating Encryption

Symmetric:

**Steal the key!**



# Defeating Encryption

Symmetric:

Steal the key!

```
cy -f /root/physmem.bin truecryptsummary
latility Framework 2.4
eCrypt Version 7.0a
eCrypt.exe at 0xff95fda0 pid 1892
ecrypt state SERVICE_RUNNING
ecrypt.sys at 0xfbfb40000 - 0xfbfb77000
-> \Device\TrueCryptVolumeZ mounted 2010-12-29
me{06e5b692-138f-11e0-a461-0003ffa616b5} -> \D
ounted 2010-12-29 21:19:32 UTC+0000
-> \Device\TrueCryptVolumeZ mounted 2010-12-29
lver\truecrypt at 0x103d030 range 0xfbfb40000 -
eCryptVolumeZ at 0x811405f0 type FILE_DEVICE_DI
n: \??\C:\Documents and Settings\Administrator\
eCrypt at 0x810caf10 type FILE_DEVICE_UNKNOWN
```



# Defeating Encryption

Asymmetric:

**Steal the key!**



Computer



id-rsa.ppk



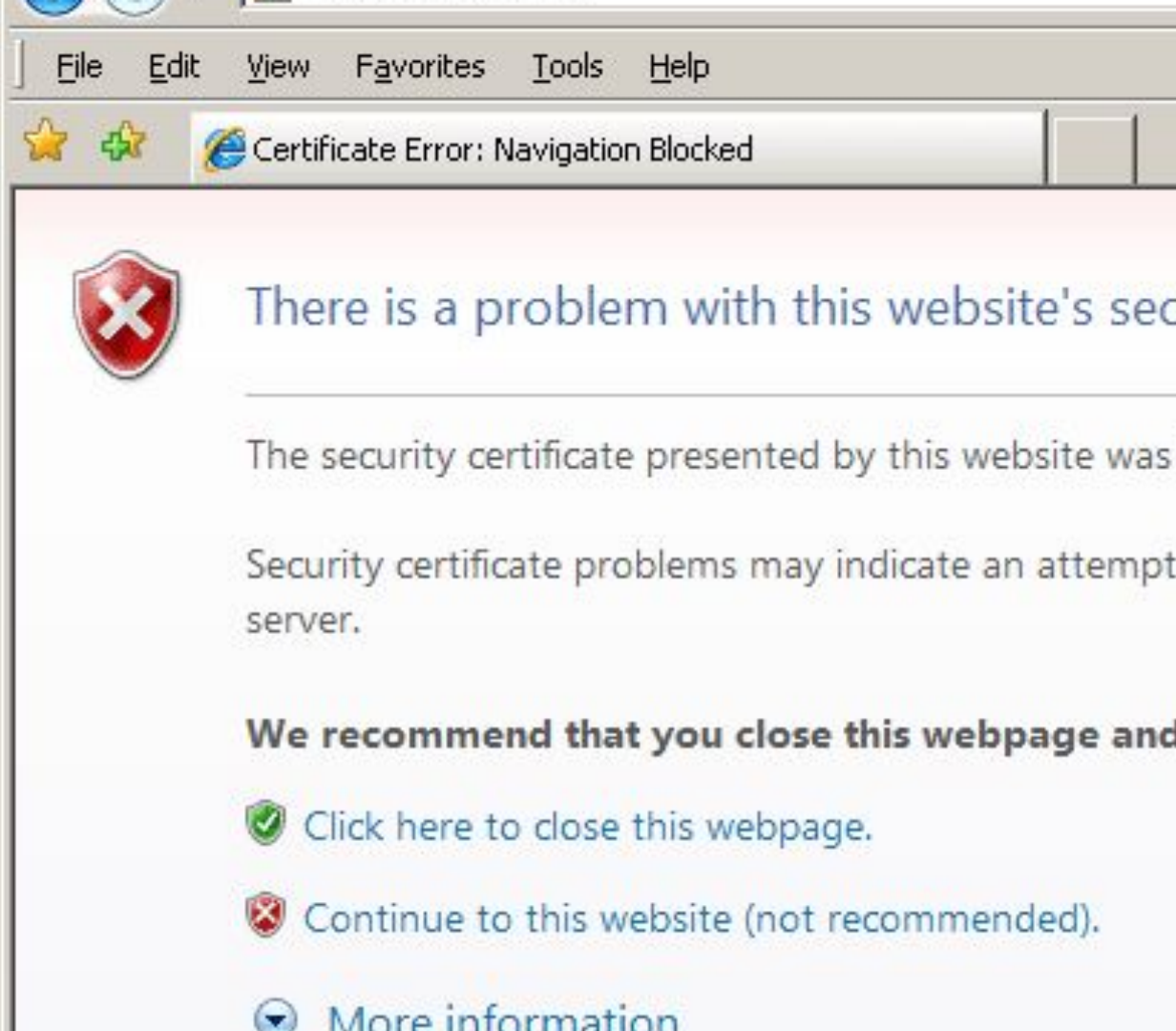
Recycle Bin



# Defeating Encryption

Asymmetric:

**Man in the middle**



# Encryption - Best Practices

**Protect your keys!!!**

**Strong** keys and  
cipher suites

**Patch** your crypto  
libraries

# Thanks!

Justin Hall

justin.hall@cbts.net | @justinhall