

Example Use of Ciphers: Wireless LAN

- WEP
 - RC4, 40-bit key, 24-bit IV
 - RC4, 104-bit key, 24-bit IV
 - (Weakness in RC4 if known IV used and keystream known)
- WPA2:
 - AES, Counter Mode, 128-bit key, 128-bit block

Example Use of Ciphers: Disk Encryption

- Linux, e.g. Ubuntu
 - dm-crypt, LUKS: AES, 256-bit key, CBC
- Mac OS X
 - FileVault 2: AES, 128-bit key, XTS
- Windows
 - BitLocker: AES, 128-bit key, CBC

Example Use of Ciphers: Internet

- Web Browsing, Remote Login, etc.
 - Use SSL/TLS
 - Depends on client (e.g. Firefox) and server (e.g. Apache)
 - Eg. capture from Firefox to Google.co.th

```
Frame 28: 235 bytes on wire (1880 bits), 235 bytes captured (1880 bits)
Ethernet II, Src: 8c:a9:82:b1:38:90, Dst: 00:23:69:3a:f4:7d
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 74.125.135.94
Transmission Control Protocol, Src Port: 48648, Dst Port: 443, Seq: 1, Ack: 1
Secure Sockets Layer
```

```
  TLSv1 Record Layer: Handshake Protocol: Client Hello
```

```
    Content Type: Handshake (22)
```

```
    Version: TLS 1.0 (0x0301)
```

```
    Handshake Protocol: Client Hello
```

```
      Cipher Suites (36 suites)
```

```
        Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
```

```
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
```

```
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
```

```
        Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
```

```
        Cipher Suite: TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)
```

```
        Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

```
        Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
```

```
        Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
```

```
        Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
```

```
        Cipher Suite: TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
```

```
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

```
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
```

```
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
```

```
        Cipher Suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
```

```
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
```

```
        Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
```

```
        Cipher Suite: TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)
```

```
        Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
```

```
        Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
```

```
        Cipher Suite: TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
```

```
        Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
```

```
        Cipher Suite: TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
```

Frame 30: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits)
Ethernet II, Src: 00:23:69:3a:f4:7d, Dst: 8c:a9:82:b1:38:90
Internet Protocol Version 4, Src: 74.125.135.94, Dst: 192.168.1.8
Transmission Control Protocol, Src Port: 443, Dst Port: 48648, Seq: 1, Ack: 170
Secure Sockets Layer
 TLsv1 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 92
 Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 88
 Version: TLS 1.0 (0x0301)
 Random
 gmt_unix_time: Dec 7, 2012 10:53:00.000000000 ICT
 random_bytes: e279c8c2da42157abbce91843e580cb8422d6c1942a7927d...
 Session ID Length: 0
 Cipher Suite: **TLS_ECDHE_RSA_WITH_RC4_128_SHA** (0xc011)
 Compression Method: null (0)