

No electronic equipment or reference material is allowed in the examination.

1. Security terminology

Give an example of each of the following:

- (a) key distribution (2p)
- (b) input sanitization (2p)
- (c) non-repudiation (2p)

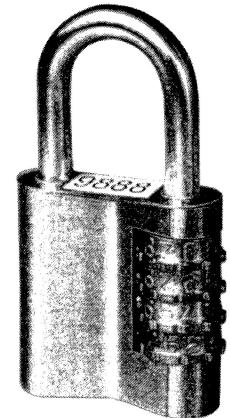
Please answer each item with one sentence. Please try to give representative, concrete, real-world examples. No definitions or general explanations.

2. Authentication

A mechanical combination lock has between 3 and 6 wheels, each with the digits 0–9. To open the lock, one needs to align the wheels correctly.

- a) What is the entropy of the secret key information for the 3-wheel and 6-wheel locks?
- b) If it takes one second for a brute-force attacker to try one combination, how long will it take to open the 3-wheel and 6-wheel locks?
- c) The mechanical combination lock is replaced with a new electronic design, which has the same external appearance but an electronic mechanism inside. How could the security of the electronic lock be improved compared to the mechanical one? No network or radio communication can be used.

It is sufficient to perform the numerical calculations approximately but please write down your calculations.



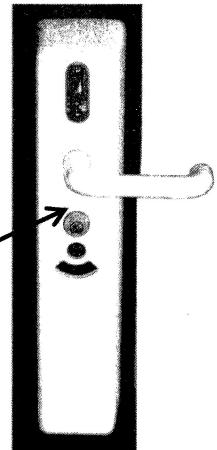
Please turn the
paper for the
remaining problems.

3. Threat analysis

What security threats are there against coin locks on public toilets? Additionally, prioritize the most important threats.

(6p)

To open,
insert 1€
coin, then
turn handle



4. Data encryption

You are travelling with a laptop that has BitLocker encryption enabled for the hard disk. The laptop has a built-in TPM security module. When you start up the laptop, it goes directly to the Windows login screen (without asking for a boot PIN and without requiring the insertion of a hardware key).

At the Elbonian airport, an officer takes your powered-down laptop to a back office to be examined while his colleague spends an hour interrogating you about your travel plans. Then, they return the laptop to you and let you go.

Question: In what different ways could Elbonian secret police have gained access to the data on your laptop?

(6p)

5. Network security

In appendix 1, there is a pretty-printed certificate chain. Explain in detail how the web browser checks the certificate chain and how it is used to authenticate the web site in SSL or TLS.

Notes: You do not need to explain the details of the TLS handshake protocol. Also, “rsaEncryption” in this context means the RSA algorithm for any purpose, which may be encryption or signature.

(6p)

Appendix 1

Certificate:

Data:

Version: 3 (0x2)
Serial Number:
0c:e7:e0:e5:17:d8:46:fe:8f:e5:60:fc:1b:f0:30:39
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA
Validity
Not Before: Nov 10 00:00:00 2006 GMT
Not After : Nov 10 00:00:00 2031 GMT
Subject: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ad:0e:15:ce:e4:43:80:5c:b1:87:f3:b7:60:f9:
71:12:a5:ae:dc:26:94:88:aa:f4:ce:f5:20:39:28:
58:60:0c:f8:80:da:a9:15:95:32:61:3c:b5:b1:28:
84:8a:8a:dc:9f:0a:0c:83:17:7a:8f:90:ac:8a:e7:
79:53:5c:31:84:2a:f6:0f:98:32:36:76:cc:de:dd:
3c:a8:a2:ef:6a:fb:21:f2:52:61:df:9f:20:d7:1f:
e2:b1:d9:fe:18:64:d2:12:5b:5f:f9:58:18:35:bc:
47:cd:a1:36:f9:6b:7f:d4:b0:38:3e:c1:1b:c3:8c:
33:d9:d8:2f:18:fe:28:0f:b3:a7:83:d6:c3:6e:44:
c0:61:35:96:16:fe:59:9c:8b:76:6d:d7:f1:a2:4b:
0d:2b:ff:0b:72:da:9e:60:d0:8e:90:35:c6:78:55:
87:20:a1:cf:e5:6d:0a:c8:49:7c:31:98:33:6c:22:
e9:87:d0:32:5a:a2:ba:13:82:11:ed:39:17:9d:99:
3a:72:a1:e6:fa:ad:d9:17:31:75:ae:85:7d:22:
ae:3f:01:46:86:f6:28:79:c8:b1:da:e4:57:17:c4:
7e:1c:0e:b0:b4:92:a6:56:b3:bd:b2:97:ed:aa:a7:
f0:b7:c5:a8:3f:95:16:d0:ff:a1:96:eb:08:5f:18:
77:4f
Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Subject Key Identifier:
45:EB:A2:AF:F4:92:CB:82:31:2D:51:8B:A7:A7:21:9D:F3:6D:C8:0F
X509v3 Authority Key Identifier:
keyid:45:EB:A2:AF:F4:92:CB:82:31:2D:51:8B:A7:A7:21:9D:F3:6D:C8:0F
Signature Algorithm: sha1WithRSAEncryption
a2:0e:bc:df:e2:ed:f0:3:72:73:7a:64:94:bf:f7:72:66:d8:
32:e4:42:75:62:ae:87:eb:f2:d5:d9:de:56:b3:9f:cc:ce:14:
28:b9:0d:97:60:5c:12:4c:58:e4:d3:d3:83:49:45:58:97:35:
69:1a:a8:47:ea:56:c6:79:ab:12:d8:67:81:84:df:7f:09:3c:
94:e6:b8:26:2c:20:bd:3d:b3:28:89:f7:f5:ff:22:e2:97:84:
1f:e9:65:ef:87:0:df:c1:67:49:b3:5d:eb:b2:09:2a:eb:26:
ed:78:be:7d:3f:2b:f3:b7:26:35:6d:5f:89:01:b6:49:5b:9f:
01:05:9b:ab:3d:25:c1:cc:b6:7f:c2:f1:6f:86:c6:fa:64:68:
eb:81:2d:94:eb:42:b7:fa:8c:le:dd:62:f1:be:50:67:b7:6c:
bd:f3:f1:if:6b:0c:36:07:16:f7:37:c1:a9:5b:6d:7a:f1:12:
46:60:83:d7:27:04:be:4b:ce:97:be:c3:67:2a:68:11:f0:80:
e7:0c:33:66:bf:13:0d:14:6e:f3:7f:1f:63:10:1e:fa:8d:1b:
25:6d:6c:8f:a5:b7:61:01:b1:d2:a3:26:a1:10:71:9d:ad:e2:
c3:f9:c3:99:51:b7:2b:07:08:ce:2e:e6:50:b2:a7:fa:0a:45:
2f:a2:f0:f2

Certificate:

Data:

Version: 3 (0x2)
Serial Number:
08:70:bc:c5:af:3f:db:95:9a:91:cb:6a:ee:ef:e4:65
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA
Validity
Not Before: Nov 18 12:00:00 2014 GMT
Not After : Nov 18 12:00:00 2024 GMT
Subject: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:c5:76:0f:0f:d:43:29:3b:6c:6d:d1:47:ad:de:
10:bf:23:c2:78:a8:4a:77:35:f1:23:5b:e0:4c:1e:
41:e7:c2:31:00:bd:88:37:45:75:dd:b9:02:10:80:
1e:8f:ed:64:23:04:45:a7:a0:39:3b:81:4d:cf:63:
3f:c2:49:ff:22:9e:88:b0:d2:96:b9:5c:8a:74:1f:
92:2a:2a:f2:12:c8:b7:68:54:b5:58:41:81:40:68:
06:1a:4f:85:29:fb:b5:4d:3c:0f:4f:3f:40:96:1b:
ce:a8:cc:5e:35:ff:64:98:f5:7d:74:54:05:a0:
36:11:04:12:24:55:63:ef:94:77:2e:77:f1:15:76:
ee:d3:a4:59:45:21:9f:a8:be:d1:27:ed:0a:8e:ab:
38:ca:3f:87:d1:da:f1:8f:b9:0b:1f:44:e7:e0:ad:
f3:95:c2:16:4d:ec:84:a3:3a:92:d4:cf:c6:7d:e6:
bd:cb:1a:40:4f:b3:54:bl:f3:8f:6f:0d:1e:e3:be:
49:a3:56:e4:07:bc:8d:a7:ce:ld:b0:5b:57:56:di:
c4:1c:fc:98:65:d1:cd:46:2f:91:94:bf:45:85:49:
f8:6d:52:87:1c:02:56:01:01:27:16:ab:72:2e:f4:71:
e4:61:b5:20:a0:fa:26:69:6a:0a:f1:ab:9f:6d:b7:
cf:25
Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
Authority Information Access:
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
X509v3 CRL Distribution Points:
Full Name:
URI:http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl
Full Name:

URI:<http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl>
X509v3 Certificate Policies:
 Policy: X509v3 Any Policy
 CPS: <https://www.digicert.com/CPS>
X509v3 Subject Key Identifier:
 67:FD:88:20:14:27:98:C7:09:D2:25:19:BB:E9:51:11:63:75:50:62
X509v3 Authority Key Identifier:
 keyid:45:EB:A2:AF:F4:92:CB:82:31:2D:51:8B:A7:A7:21:9D:F3:6D:C8:0F
Signature Algorithm: sha256WithRSAEncryption
 a9:28:35:7a:c4:7b:a6:da:27:1e:ac:98:c7:27:36:4f:11:32:
 74:74:4e:40:d1:d1:cd:f2:68:77:35:af:b3:8c:5d:c6:04:bf:
 15:f4:23:67:8b:b9:6f:97:04:eb:46:9d:c2:cd:c9:d1:a4:ae:
 81:2e:c9:ba:b1:e8:80:d0:1c:c9:39:c1:56:76:59:6c:9c:7d:
 e3:a9:f0:d3:d1:34:48:3c:49:59:8b:1a:98:ce:bf:c6:f2:d8:
 30:35:ff:9e:6f:5d:a0:af:3a:ee:66:53:ae:a8:c9:69:c8:be:
 9a:a7:a0:7b:d8:82:4b:33:13:c8:07:f3:77:d7:f3:64:cd:9e:
 63:f9:42:27:53:ae:10:33:89:72:37:15:f1:be:f7:1e:35:a2:
 ce:33:2d:f2:7t:b2:e6:0b:7:69:0e:51:f5:7c:69:9b:7e:
 ce:26:1a:33:44:c3:ba:77:05:3b:ba:5d:3f:41:89:fa:16:3b:
 ee:04:6e:5b:ac:56:4b:ef:8c:70:f2:4a:7b:57:bd:19:6e:8b:
 36:07:54:26:2d:86:09:94:1f:5f:37:ab:f0:23:3f:8f:2c:5f:
 96:9e:47:71:a8:44:de:a9:b9:85:2f:b5:34:60:a5:5f:09:a0:
 9a:43:id:d4:bf:2d:44:d6:8d:da:fd:75:cb:5f:16:a0:0e:61:
 c2:70:3d:36

Certificate:
Data:
 Version: 3 (0x2)
 Serial Number:
 02:72:71:c2:fe:ca:5c:4e:3b:1c:cc:a8:67:97:c4:1e
Signature Algorithm: sha256WithRSAEncryption
 Issuer: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
Validity
 Not Before: Jan 15 00:00:00 2016 GMT
 Not After : Jan 23 12:00:00 2019 GMT
 Subject: C=FI, ST=Uusimaa, L=Espoo, O=Aalto University Foundation, OU=Department of Computer Science, CN=www.cs.hut.fi
Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
Modulus:
 00:ce:7a:5c:cd:45:da:fb:51:db:8f:13:fb:ea:39:
 cd:3f:db:e6:18:45:8d:75:12:b6:38:a8:be:df:4f:
 5c:c0:42:2c:1a:7a:d4:ca:d5:35:ff:3:3:f3:a5:7f:
 a9:71:df:2e:95:c8:3e:cb:9e:b9:e1:22:b8:70:7c:
 7f:f4:9c:67:61:da:a6:01:56:8a:f4:e5:97:01:9f:
 dc:dc:4a:2b:36:f7:91:0e:fe:a9:3:91:c3:cf:0b:
 22:94:bf:55:ea:de:d4:cb:8c:7:f4:5:f:4e:3:c:7:
 16:30:d6:5a:c3:fe:ab:71:39:a0:d9:2b:f7:6e:54:
 7a:8c:c3:e6:c5:59:37:3d:51:40:66:36:38:2b:4d:
 7d:a6:c2:5f:f8:67:a1:d9:07:1f:c6:2e:01:ba:b3:
 a8:52:a5:8e:b8:da:48:3a:2d:e7:3a:d4:ee:e7:d5:
 fe:d6:06:f5:9e:50:bd:d3:99:2a:65:7e:09:74:0f:
 40:d7:87:e3:bc:0f:39:90:69:7f:8c:1a:af:le:8b:
 88:e9:4f:99:29:f4:4b:14:36:f3:ee:46:32:91:ca:
 37:ea:21:37:ef:13:f2:99:42:ad:f3:93:2c:97:1f:
 26:84:7c:73:00:27:ad:cf:fe:bb:10:6e:e9:b3:29:
 c4:dd:f4:f1:56:21:95:e1:2f:96:8a:76:bf:89:6e:
 52:3b
 Exponent: 65537 (0x10001)

X509v3 extensions:
X509v3 Authority Key Identifier:
 keyid:67:FD:88:20:14:27:98:C7:09:D2:25:19:BB:E9:51:11:63:75:50:62
X509v3 Subject Key Identifier:
 DD:21:81:30:50:E5:D6:D2:E7:1F:8C:BB:C5:0C:31:C7:60:50:C4:91
X509v3 Subject Alternative Name:
 DNS:www.cs.hut.fi, DNS:www.cse.tkk.fi
X509v3 Key Usage:
 Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
 TLS Web Server Authentication, TLS Web Client Authentication
X509v3 CRL Distribution Points:
Full Name:
 URI:<http://crl3.digicert.com/TERENASSLCA3.crl>
Full Name:
 URI:<http://crl4.digicert.com/TERENASSLCA3.crl>
X509v3 Certificate Policies:
 Policy: 2.16.840.1.114412.1.1
 CPS: <https://www.digicert.com/CPS>
 Policy: 2.23.140.1.2.2
Authority Information Access:
 OCSP - URI:<http://ocsp.digicert.com>
 CA Issuers - URI:<http://cacerts.digicert.com/TERENASSLCA3.crt>
X509v3 Basic Constraints: critical
CA:FALSE
Signature Algorithm: sha256WithRSAEncryption
 88:25:ff:0c:a6:6d:55:01:b3:fc:64:35:16:c5:56:c4:e1:bb:
 0e:94:83:85:07:7a:6c:96:2e:50:6a:8a:b9:8c:00:a9:c8:f9:
 ba:cc:6e:ec:da:ab:0a:e3:77:c0:d8:f6:91:d2:b2:8e:7a:5b:
 4c:1c:e5:82:d1:49:a0:95:e3:c8:d4:d8:ce:62:59:43:b3:db:
 d6:ee:6:c9:ad:e3:63:d2:24:d7:d6:49:a8:20:92:df:01:79:03:
 d2:54:93:98:06:eo:cd:13:79:29:ea:a6:9c:63:83:37:06:3f:
 36:71:ed:a4:62:54:ec:b4:61:40:41:f1:66:3f:32:3c:f0:33:
 98:4b:84:43:d0:0:ce:08:71:51:8e:32:66:64:4f:cfc:41:d7:
 e0:ac:53:fe:ib:5:cd:f2:5a:43:19:69:b7:f4:7a:c8:b2:fb:57:
 54:1b:ab:04:ce:18:e6:54:1c:52:d0:a6:7a:ad:db:43:ac:82:
 ad:37:71:d3:be:4e:97:26:0e:9a:8e:3f:c6:0e:52:bc:fa:ib:
 f7:91:01:d9:cf:36:e5:72:58:29:6f:fb:29:6b:78:87:98:49:
 85:42:3a:ea:57:09:2a:92:52:2a:c2:18:11:1a:ef:62:29:65:
 de:5a:47:7b:49:41:d0:ee:c5:a6:73:0a:9f:f2:14:ed:95:1b:
 b0:b6:7f:8c