SECURITY IN ELECTRONIC COMMERCE

Final exam OpenCourseWare

Name:

MULTIPLE-CHOICE QUESTIONS

Each question has only one correct answer, which ought to be clearly pointed out with an 'X'. Each question incorrectly answered will be evaluated as minus one third of the mark obtained had it been correctly answered.

1.- Time stamping authorities:

- □ Need to know the contents of the message to issue its time stamp.
- □ May issue the time stamp by concatenating the message with the date and time.
- □ Take the date and time data from a trusted source.

2.- The set of specifications developed by the IETF PKIX group:

- □ They are the same that the ones developed by ISO/IEC under the X.509 identifier.
- □ One of them follows partially the ISO/IEC X.509 Recommendation.
- □ None of them is based on the ISO/IEC X.509 Recommendation.

3. - The purpose of the specification ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) is:

- □ To define a set of XML formats for the signatures used in the SET protocol
- □ To define a set of XML formats for signatures that remain valid over long periods
- □ To define a set of XML formats for signatures that must be used to create electronic invoices

4.- SSL:

- □ Does not allow data compression.
- □ Supports RSA and DH as public key algorithms.
- □ SSL acceleration is usually performed at client's side to make up for its usually less computing power.

5.- SET:

- □ It is relatively simple and has a low consumption of computer resources.
- □ Demands all the participants to have an X.509 public-key certificate.
- □ Simplifies the process of authenticating the client by using a password instead of public key certificates.

6.- 3D-Secure:

- □ Uses the mechanism known as dual signature to provide non-repudiation.
- □ Requires the merchant and the buyer to install specific software.
- □ Helps issuer to verify that the person making an e-commerce purchase is an authorized cardholder.

SECURITY IN ELECTRONIC COMMERCE

Final exam OpenCourseWare

Name:

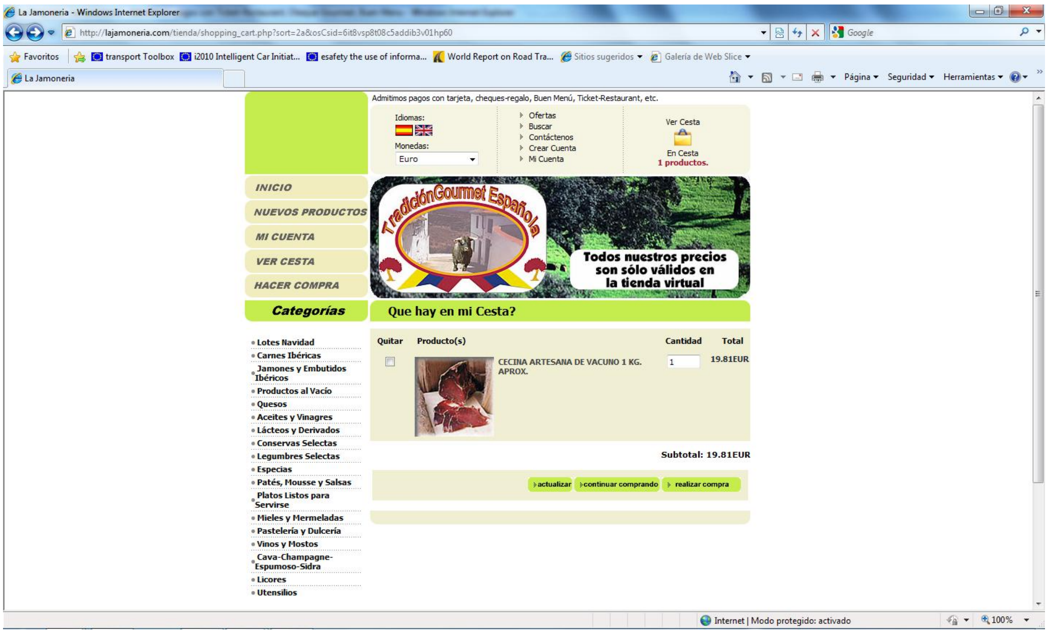
Question 1 . Next figures show the different steps of the purchase process followed in certain virtual shop. Answer the following questions:

a. Mention existing security elements and assess the global security level that a typical user may sense.

b. List security services (not protocols) that have not been considered in this process (a maximum of three). Explain why they are important.

c. Do you miss the mandatory mention of some law?

d. Enumerate a maximum of five issues not specifically related to security that have an influence on the sensed security/insecurity. Do you miss some external endorsement that may help to increase the potential buyer's trust?



La Jamoneria - Windows Internet Explorer
http://lajamoneria.com/tienda/shopping_cart.php?sort=2a&osCsid=6it8vsp8t08c5addib3v01hp60
Google
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
La Jamoneria
Página
Seguridad
Herramientas
Tradición Gourmet Española
Internet | Modo protegido: activado
100%

Admitimos pagos con tarjeta, cheques-regalo, Buen Menú, Ticket-Restaurant, etc.

Idiomas:

Monedas: Euro

- Ofertas
- Buscar
- Contáctenos
- Crear Cuenta
- Mi Cuenta

Ver Cesta

En Cesta
1 productos.

INICIO

NUEVOS PRODUCTOS

MI CUENTA

VER CESTA

HACER COMPRA

Todos nuestros precios son sólo válidos en la tienda virtual

Categorías

- Lotes Navidad
- Carnes Ibéricas
- Jamones y Embutidos Ibéricos
- Productos al Vacío
- Quesos
- Aceites y Vinagres
- Lácteos y Derivados
- Conservas Selectas
- Legumbres Selectas
- Especias
- Patés, Mousse y Salsas
- Platos Listos para Servirse
- Mieles y Mermeladas
- Pastelería y Dulcería
- Vinos y Mostos
- Cava-Champagne-Espumoso-Sidra
- Licores
- Utensilios

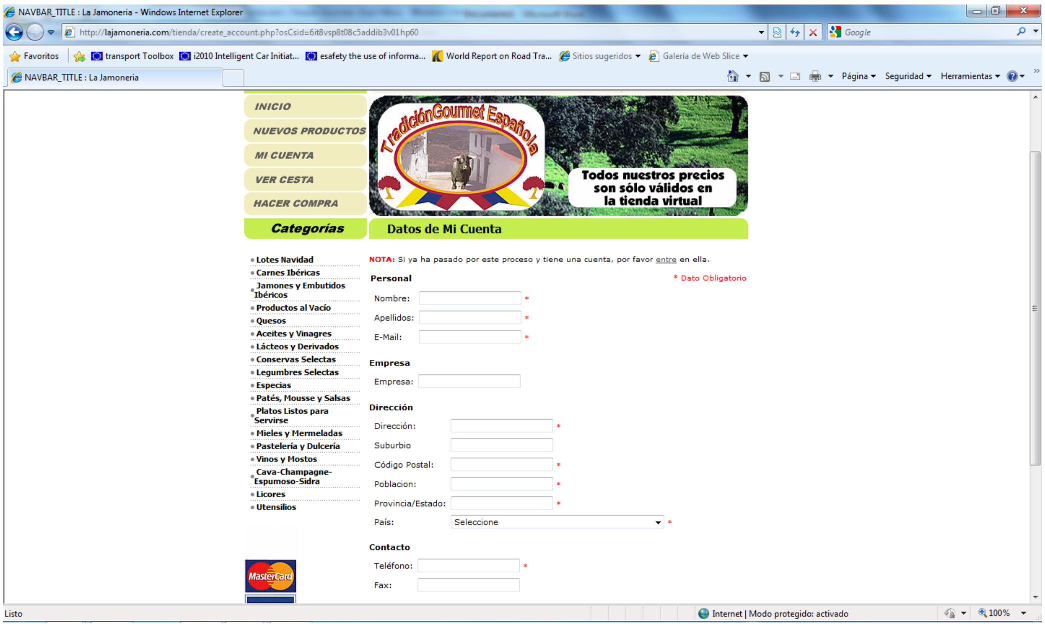
Que hay en mi Cesta?

Quitar	Producto(s)	Cantidad	Total
□	CECINA ARTESANA DE VACUNO 1 KG. APROX.	1	19.81EUR

Subtotal: 19.81EUR

actualizar | continuar comprando | realizar compra

Figure 1. Product information


NAVBAR_TITLE : La Jamoneria - Windows Internet Explorer
http://lajamoneria.com/tienda/create_account.php?osCsid=6it8vsp8t08c5addib3v01hp60
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
NAVBAR_TITLE : La Jamoneria
Página
Seguridad
Herramientas
INICIO
NUEVOS PRODUCTOS
MI CUENTA
VER CESTA
HACER COMPRA
TradiciónGourmet Española
Todos nuestros precios son sólo válidos en la tienda virtual
Categorías
MasterCard
Listo
Internet | Modo protegido: activado
100%

Categorías

- Lotes Navidad
- Carnes Ibéricas
- Jamones y Embutidos Ibéricos
- Productos al Vacío
- Quesos
- Aceites y Vinagres
- Lácteos y Derivados
- Conservas Selectas
- Legumbres Selectas
- Especias
- Patés, Mousse y Salsas
- Platos Listos para Servirse
- Mieles y Mermeladas
- Pastelería y Dulcería
- Vinos y Mostos
- Cava-Champagne-Espumoso-Sidra
- Licores
- Utensilios

Datos de Mi Cuenta

NOTA: Si ya ha pasado por este proceso y tiene una cuenta, por favor entre en ella.

Personal * Dato Obligatorio

Nombre: *

Apellidos: *

E-Mail: *

Empresa

Empresa:

Dirección

Dirección: *

Suburbio

Código Postal: *

Poblacion: *

Provincia/Estado: *

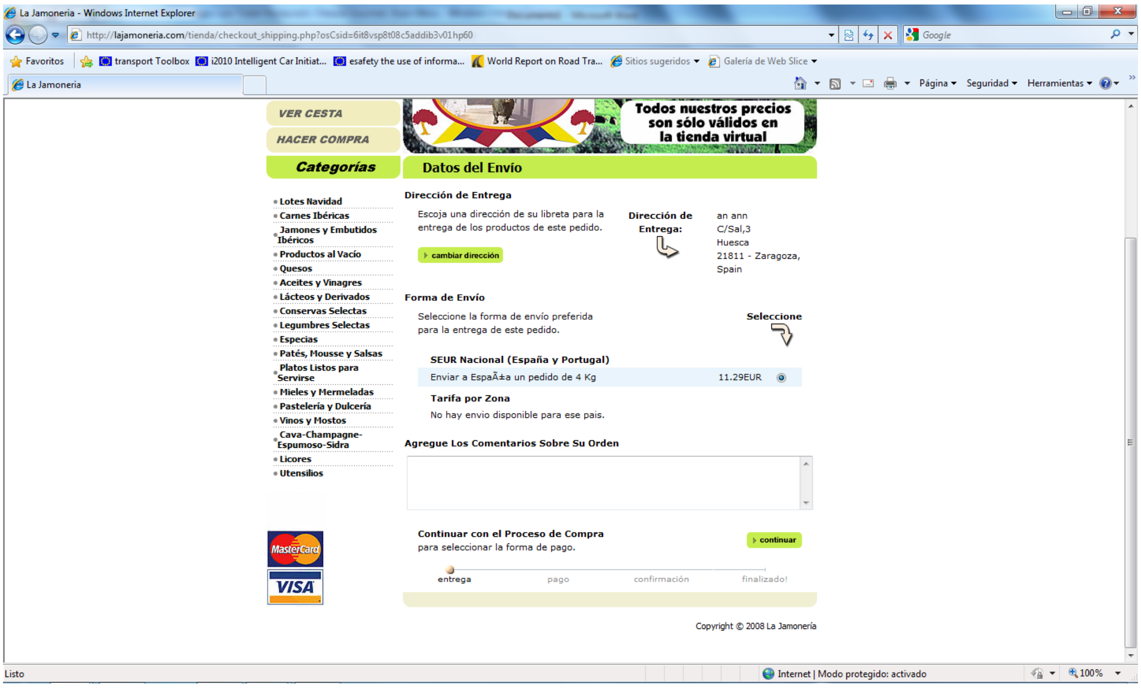
País: Seleccione *

Contacto

Teléfono: *

Fax:

Figure 2. Purchase process, step 1. Creation of an account.


La Jamoneria - Windows Internet Explorer
http://lajamoneria.com/tienda/checkout_shipping.php?osCsid=6it8vsp8t08c5addib3v01hp60
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
La Jamoneria
Página
Seguridad
Herramientas
VER CESTA
HACER COMPRA
Todos nuestros precios son sólo válidos en la tienda virtual
Categorías
MasterCard
VISA
cambiar dirección
continuar
Listo
Internet | Modo protegido: activado
100%

Categorías

- Lotes Navidad
- Carnes Ibéricas
- Jamones y Embutidos Ibéricos
- Productos al Vacío
- Quesos
- Aceites y Vinagres
- Lácteos y Derivados
- Conservas Selectas
- Legumbres Selectas
- Especias
- Patés, Mousse y Salsas
- Platos Listos para Servirse
- Mieles y Mermeladas
- Pastelería y Dulcería
- Vinos y Mostos
- Cava-Champagne-Espumoso-Sidra
- Licores
- Utensilios

Datos del Envío

Dirección de Entrega

Escoja una dirección de su libreta para la entrega de los productos de este pedido.

Dirección de Entrega:

an ann
C/Sal,3
Huesca
21811 - Zaragoza,
Spain

Forma de Envío

Seleccione la forma de envío preferida para la entrega de este pedido. Seleccione

SEUR Nacional (España y Portugal)

Enviar a EspaÃ±a un pedido de 4 Kg 11.29EUR ●

Tarifa por Zona

No hay envio disponible para ese pais.

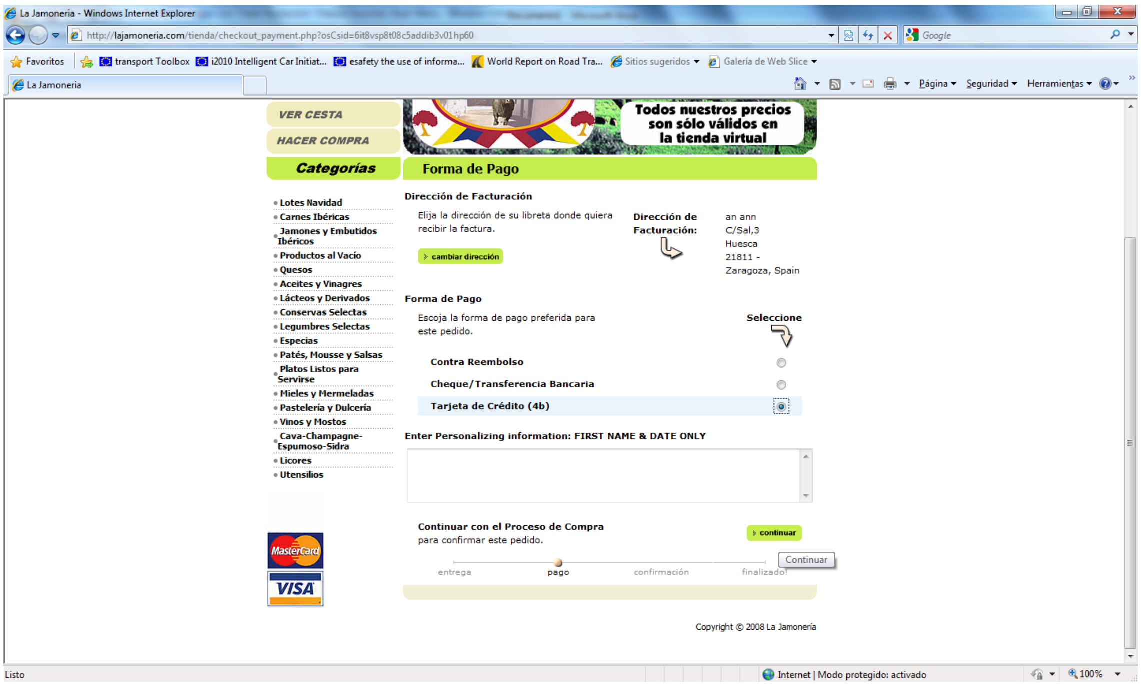
Agregue Los Comentarios Sobre Su Orden

Continuar con el Proceso de Compra para seleccionar la forma de pago.

entrega pago confirmación finalizado!

Copyright © 2008 La Jamonería

Figure 3. Purchase process, step 2. Confirmation of delivery information



Forma de Pago

Dirección de Facturación

Elija la dirección de su libreta donde quiera recibir la factura.

Dirección de Facturación:

an ann
C/Sal,3
Huesca
21811 -
Zaragoza, Spain

Forma de Pago

Escoja la forma de pago preferida para este pedido.

Seleccione

Contra Reembolso ○

Cheque/Transferencia Bancaria ○

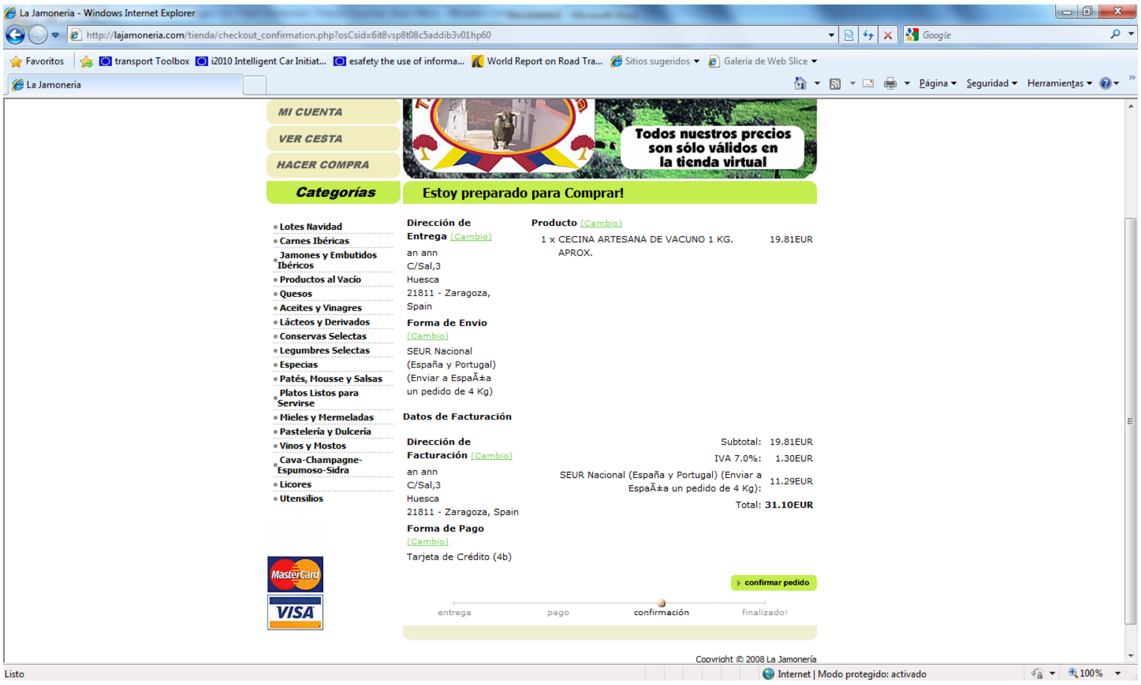
Tarjeta de Crédito (4b) ●

Enter Personalizing information: FIRST NAME & DATE ONLY

Continuar con el Proceso de Compra
para confirmar este pedido.

Copyright © 2008 La Jamonería

Figure 4. Purchase process, step 3. Selection of payment method



Estoy preparado para Comprar!

Dirección de Entrega (Cambio)

an ann
C/Sal,3
Huesca
21811 - Zaragoza,
Spain

Forma de Envio (Cambio)

SEUR Nacional (España y Portugal) (Enviar a EspaÃ±a un pedido de 4 Kg)

Producto (Cambio)

1 x CECINA ARTESANA DE VACUNO 1 KG. APROX.	19.81EUR

Datos de Facturación

Dirección de Facturación (Cambio)

an ann
C/Sal,3
Huesca
21811 - Zaragoza, Spain

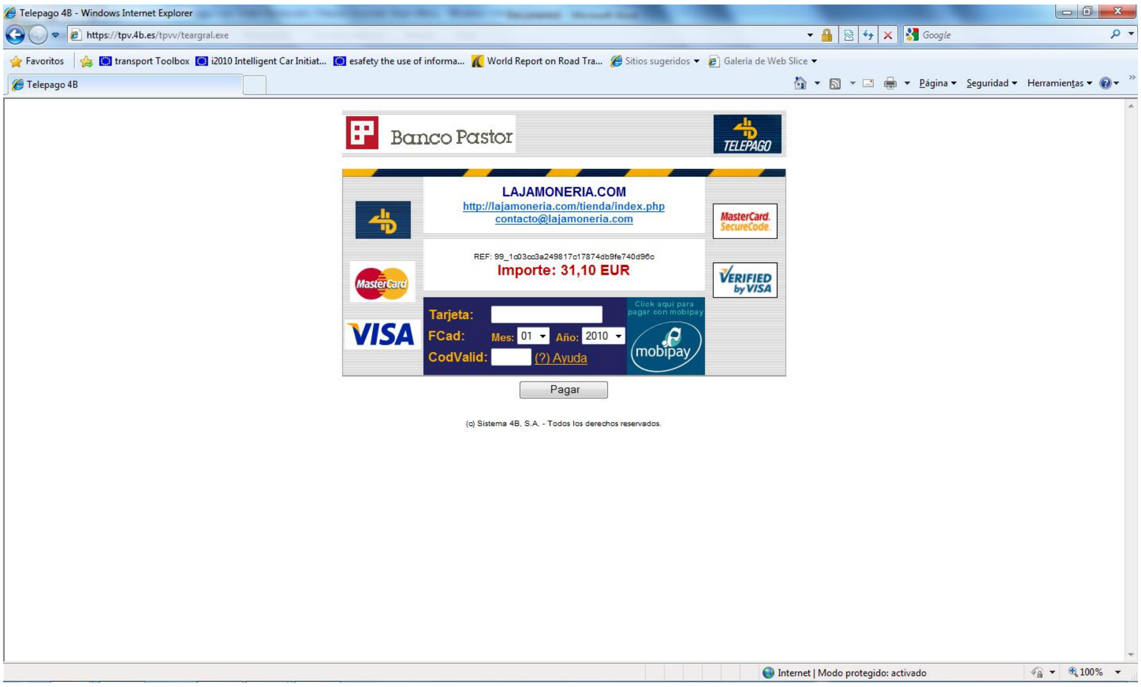
Forma de Pago (Cambio)

Tarjeta de Crédito (4b)

Subtotal:	19.81EUR
IVA 7.0%:	1.30EUR
SEUR Nacional (España y Portugal) (Enviar a EspaÃ±a un pedido de 4 Kg):	11.29EUR
Total:	**31.10EUR**

Copyright © 2008 La Jamonería

Figure 5. Purchase process, step 4. Purchase request confirmation


Telepago 4B - Windows Internet Explorer
https://tpv.4b.es/tpvv/teargral.exe
Google
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
Telepago 4B
Página
Seguridad
Herramientas
Banco Pastor
TELEPAGO
MasterCard SecureCode
MasterCard
VERIFIED by VISA
VISA
Internet | Modo protegido: activado
100%

LAJAMONERIA.COM
http://lajamoneria.com/tienda/index.php
contacto@lajamoneria.com

REF: 99_1c03cc3a249817c17874db9fe740d96c
Importe: 31,10 EUR

Tarjeta:
FCad: Mes: 01 Año: 2010
CodValid: (?) Ayuda

Click aquí para pagar con mobipay
mobipay

Pagar

(c) Sistema 4B, S.A. - Todos los derechos reservados.

Figure 6. Payment details using 4B payment system.

SECURITY IN ELECTRONIC COMMERCE

Final exam OpenCourseWare

Name:

Question 2 - Describe in detail the process that has to be followed to validate an X.509 public key certificate.

Question 3 - During the process of retrieving a web page from a web server using an SSL connection, you receive the certificate shown below. Mention several reasons to not trust this certificate. Mention also if some the used algorithms is considered insecure nowadays.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 65 (0x41)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
        Validity
            Not Before: Jul 31 00:00:00 2004 GMT
            Not After : Sep  2 00:00:00 2004 GMT
        Subject: CN=MD5 Collisions Inc. (http://www.phreedom.org/md5)
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ba:a6:59:c9:2c:28:d6:2a:b0:f8:ed:9f:46:a4:
                    a4:37:ee:0e:19:68:59:d1:b3:03:99:51:d6:16:9a:
                    5e:37:6b:15:e0:0e:4b:f5:84:64:f8:a3:db:41:6f:
                    35:d5:9b:15:1f:db:c4:38:52:70:81:97:5e:8f:a0:
                    b5:f7:7e:39:f0:32:ac:1e:ad:44:d2:b3:fa:48:c3:
                    ce:91:9b:ec:f4:9c:7c:e1:5a:f5:c8:37:6b:9a:83:
                    de:e7:ca:20:97:31:42:73:15:91:68:f4:88:af:f9:
                    28:28:c5:e9:0f:73:b0:17:4b:13:4c:99:75:d0:44:
                    e6:7e:08:6c:1a:f2:4f:1b:41
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                CRL Sign
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                A7:04:60:1F:AB:72:43:08:C5:7F:08:90:55:56:1C:D6:CE:E6:38:EB
            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6C

            Netscape Comment:
                3
    Signature Algorithm: md5WithRSAEncryption
        a7:21:02:8d:d1:0e:a2:80:77:25:fd:43:60:15:8f:ec:ef:90:
        47:d4:84:42:15:26:11:1c:cd:c2:3c:10:29:a9:b6:df:ab:57:
        75:91:da:e5:2b:b3:90:45:1c:30:63:56:3f:8a:d9:50:fa:ed:
        58:6c:c0:65:ac:66:57:de:1c:c6:76:3b:f5:00:0e:8e:45:ce:
        7f:4c:90:ec:2b:c6:cd:b3:b4:8f:62:d0:fe:b7:c5:26:72:44:
        ed:f6:98:5b:ae:cb:d1:95:f5:da:08:be:68:46:b1:75:c8:ec:
        1d:8f:1e:7a:94:f1:aa:53:78:a2:45:ae:54:ea:d1:9e:74:c8:
        76:67
```

Question 4 - Explain the circumstances that lead to a successful Lebanese Loop attack at an ATM. What countermeasures can be applied?

SECURITY IN ELECTRONIC COMMERCE

Final exam OpenCourseWare

Name:

Problem 1 The protocol 3-D Secure by VISA™ allows the payment within e-commerce transactions. The entity known as Access Control Server (ACS) in this protocol has as main goal to authenticate the buyer in the transaction. As a result of the authentication process, the ACS sends a signed message (M1) to the merchant who verifies it. After interbank communications finish, the merchant sends the buyer an encrypted message (M2) showing the result of the purchase. As part of VISA's auditing process, we require you to check the following issues:

1. Message M1 comprises the following data items:

   a. Date: 20012010

   b. PAN: 1701001012211001

The signature algorithm is RSA.

The public key of the ACS is: K_p(ACS) = (e= 13 , n= 91)

The hash algorithm applied on the numeric data items of M1 works as follows: First, each data item is divided in groups of two digits. Then, it is calculated the sum of the set of two digits numbers identified in the previous step (for example: if data item is '4432', the resulting sum will be '76'). The hash of the complete message M1 is calculated by summing up the hashes of each data item and applying modulo operation with modulus 91.

Check if 32 is the correct signature over message M1.

2. Message M2 comprises the following data items:

   a. Date: 17

   b. Price: 18

Encrypt message M2. Take into account the following information regarding the keys:

K_p(merchant's public key) = (e= 32 , n= 64); K_v(buyer's prívate key) = (d= 37 , n= 143)

3. Forget the results obtained in the previous question of the problem. Suppose that message M2 only comprises a data item indicating the hour. Let 92 be the resulting ciphertext after encrypting message M2 using the keys previously specified in question 2. **Decrypt the ciphertext and explain briefly whether you consider reasonable or not the result of the decryption process.**

RSA operations reminder:

Sign / Decrypt: Result = M^d mod n

Verify / Encrypt: Result = M^e mod n