DCU

DUBLIN CITY UNIVERSITY

SEMESTER 1 SOLUTIONS 2015/2016

MODULE: CA4005 - Cryptography and Security Protocols

PROGRAMME(S):

CASE - BSc in Computer Applications (Sft.Eng.)
ECSA - Study Abroad (Engineering and Computing)

YEAR OF STUDY: 4,X

EXAMINERS: Dr Geoff Hamilton (Ph:5017)
Dr. Ian Pitt

TIME ALLOWED: 3 hours

INSTRUCTIONS: Answer 5 questions. All questions carry equal marks.

PLEASE DO NOT TURN OVER THIS PAGE UNTIL INSTRUCTED TO DO SO

The use of programmable or text storing calculators is expressly forbidden.
Please note that where a candidate answers more than the required number of questions, the examiner will mark all questions attempted and then select the highest scoring ones.

Requirements for this paper (Please mark (X) as appropriate)

□ *Log Tables*
□ *Graph Paper*
□ *Dictionaries*
□ *Statistical Tables*
□ *Thermodynamic Tables*
□ *Actuarial Tables*
□ *MCQ Only - Do not publish*
□ *Attached Answer Sheet*

QUESTION 1 **_[Total marks: 20]_**

1(a) [5 Marks]

Explain why padding schemes are necessary for block ciphers. Give two examples of appropriate padding schemes.

Solution:
Padding schemes are necessary because the length of plaintext is not usually a multiple of block length. Two appropriate padding schemes are:

- Append zeroes to last block and add an extra block which contains the length of the message in bits.
- Append single one and then zeroes to last block; if last block is full then create extra block starting with single one and then zeroes.

1(b) [8 Marks]

Compare and contrast the *Electronic Cook Book* (ECB) and *Ciphertext Block Chaining* (CBC) modes of operation for block ciphers with respect to the following (use diagrams if necessary):

- Encryption
- Decryption
- Error propagation
- Detection of alteration of ciphertext blocks

Solution:
This is mostly bookwork. In ECB mode, errors are not propagated beyond the block in which they occurred. In CBC mode, a single bit error will be propagated to the next block. In ECB mode, altered ciphertext blocks will not be detected, but in CBC mode they will since the previous ciphertext block is needed to decrypt the current one.

1(c) [7 Marks]

A block cipher has a block size of 64 bits. For both ECB mode and CBC mode, answer the following:

- After encrypting how many blocks would you expect to observe that two of the ciphertext blocks are identical?
- What information would the observation of identical ciphertext blocks reveal to an attacker?

Solution:
In ECB Mode, if the same plaintext block is repeated, then so is the corresponding ciphertext block. In this case, any repetitions in the plaintext will be reflected in the ciphertext. In CBC mode, if the same IV is being used, on average 2^{32} blocks would have to be observed before a cipertext block re-occurs. In this case the attacker will know that the XOR difference between the two preceding ciphertext blocks must be the same as the XOR difference between the two current plaintext blocks.

[End Question 1]

QUESTION 2 ***[Total marks: 20]***

2(a) [5 Marks]

Describe the structure of an X.509 *PKI certificate*, explaining the purpose of each field.

Solution:
An `X.509` certificate contains the following fields:

Field	**Description**
Serial Number	The serial number of this certificate. Each CA gives their certificates a unique serial number.
Issuer	The name of the CA that issued of the certificate.
Subject	The name of the owner of the public key being certified.
Validity Dates	`from` and `to` dates defining the period of validity of the certificate.
Public Key	The public key being certified.
...	...
Signature	Issuer's signature of the certificate.

2(b) [10 Marks]

Explain the concept of a *certificate path*. Describe an algorithm which can be used to validate a certificate path and extract a user's public key. Given a root CA (A), an intermediate CA (B) and a user (C), give an example of a certificate path used to certify C's public key, and the steps which would be followed to validate this path and extract the key.

Solution:
A certificate path is a list of certificates $\langle \mathcal{C}_0, \cdots, \mathcal{C}_k \rangle$ such that the signature for $\mathcal{C}_i$ was generated by the private key corresponding to the public key certified by $\mathcal{C}_{i+1}$. This forms a chain of trust from a user to the root CA within a CA hierarchy. The algorithm to validate the given certificate path and extract a user's public key where each certificate has the form $\mathcal{C}_i = \mathcal{C}[N_i, I_i, S_i, (F_i, T_i), K_i]$ is as follows:

```
if $(now < F_k)$ or $(now > T_k)$ then fail ;
if $revoked(I_k, N_k)$ then fail ;
for $i := k - 1$ downto $0$ do
begin
    if $I_i \neq S_{i+1}$ then fail ;
    if $(now < F_i)$ or $(now > T_i)$ then fail ;
    if $revoked(I_i, N_i)$ then fail ;
    if not $validSig(\mathcal{C}_i, K_{i+1})$ then fail ;
end
return $K_0$ ;
```

For the given example, the certificate path might look as follows:

$$\begin{array}{ll}\langle & \{|\mathcal{C}_0[\texttt{23}, \texttt{B}, \texttt{C}, (\texttt{Jan 2015}, \texttt{Dec 2019}), k_C^+]|\}_{k_B^-} \\ & \{|\mathcal{C}_1[\texttt{3452}, \texttt{A}, \texttt{B}, (\texttt{Jan 2014}, \texttt{Dec 2018}), k_B^+]|\}_{k_A^-} \\ & \{|\mathcal{C}_2[\texttt{2735}, \texttt{A}, \texttt{A}, (\texttt{Jan 2000}, \texttt{Dec 2020}), k_A^+]|\}_{k_A^-} \quad \rangle\end{array}$$

The steps which would be used to extract C's public key are as follows:

```
**if** $(now < Jan\ 2000)$ **or** $(now > Dec\ 2020)$ **then fail**
**if** $revoked(A, 2735)$ **then fail**
**if** $A \neq A$ **then fail**
**if** $(now < Jan\ 2014)$ **or** $(now > Dec\ 2018)$ **then fail**
**if** $revoked(A, 3452)$ **then fail**
**if not** $validSig(\mathcal{C}_1, K_A)$ **then fail**
**if** $B \neq B$ **then fail**
**if** $(now < Jan\ 2015)$ **or** $(now > Dec\ 2019)$ **then fail**
**if** $revoked(B, 23)$ **then fail**
**if not** $validSig(\mathcal{C}_0, K_B)$ **then fail**
**return** $K_C^+$
```

2(c) [5 Marks]

Explain the concept of a *certificate revocation list*, and why these are necessary. For the example in part (b), what CRLs are needed to validate C's certificate?

Solution:
A certificate revocation list is a list of the serial numbers of the certificates issued by the CA that have been revoked. These are necessary if the certificate has been compromised or is no longer in use. For the example in part (b), CRLs are needed for CAs A and B.

[End Question 2]

QUESTION 3 ***[Total marks: 20]***

3(a) [7 Marks]

Describe in detail how the RSA cryptosystem works. Your description should include how public and private key pairs are generated, how encryption and decryption are performed, and the hard problem that the security of RSA rests upon.

Solution:
Key generation works as follows:

- Generate two large primes p and q of at least 512 bits.
- Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$
- Select a random integer e, $1 < e < \phi(N)$, such that $\gcd(e, \phi(N)) = 1$.
- Using the extended Euclidean algorithm compute the unique integer d, $1 < d < \phi(N)$ with $ed \equiv 1 \pmod{\phi(N)}$.
- Public key is (e, N).
- Private key is (d, N).

Encryption of message m $(0 < m < N)$ is performed by computing $c = m^e \pmod N$

Decryption of ciphertext c is performed by computing $m = c^d \pmod N$

Breaking RSA can be shown to be no harder than integer factorisation.

3(b) [6 Marks]

Describe an efficient algorithm which can be used to implement encryption and decryption in RSA. Show how encryption can be implemented more efficiently by using an appropriate value for the encryption exponent. Show how decryption can be implemented more efficiently using the prime factors of the modulus.

Solution:
Encryption and decryption in RSA is done by performing modular exponentiation. An efficient algorithm for this modular exponentiation is the square and multiply algorithm; this can be computed bit by bit left-to-right or right-to-left. The left-to-right variant for computing $y = a^x \pmod{N}$ where x has n bits $x_{n-1} \dots x_0$ is as follows:

```
y = 1
for i = n-1 downto 0 do
   y = (y*y) mod N
   if $x_i$ = 1 then
      y = (y*a) mod N
   end
end
```

The encryption exponent can be chosen such that few bits are set (e.g. $65537 = 2^{16} + 1$), and thus modular multiplication will be more efficient because less multiplications will be required using the square and multiply algorithm. The decryption exponent is dependent on the encryption exponent, so cannot be selected for efficiency in this way. The Chinese Remainder Theorem can be used to perform decryption more efficiently using the prime factors of the modulus.

3(c) [7 Marks]

Suppose we have three RSA users with the same encryption exponent $e = 3$ but different public moduli N_1, N_2 and N_3. If the same message is encrypted using the public key of each of these users and sent to them, show how an attacker can use the values of these ciphertexts to recover the original message. If the values of these public moduli are $N_1 = 33$, $N_2 = 35$ and $N_3 = 39$ and the attacker sees the corresponding ciphertexts $c_1 = 31$, $c_2 = 29$ and $c_3 = 25$, determine the value of the original message. What lessons can be learned from this in improving the security of RSA?

Solution:
We use the Chinese Remainder Theorem to determine that $m^3 = 64$, so $m = 4$.

This shows that plaintexts should be randomised before applying RSA.

[End Question 3]

QUESTION 4 ***[Total marks: 20]***

4(a) [8 Marks]

Describe in detail how *Diffie-Hellman* (DH) key exchange works. Give an example with suitable small values.

Solution:
Given a prime modulus p and a generator g, Diffie-Hellman key exchange works as follows:

1. A chooses a random x such that $1 < x < p - 1$.
2. $A \rightarrow B : g^x \pmod{p}$
3. B chooses a random y such that $1 < y < p - 1$.
4. $B \rightarrow A : g^y \pmod{p}$
5. A computes $K = (g^y)^x \pmod{p}$.
6. B computes $K = (g^x)^y \pmod{p}$.
7. A and B now share the secret K.

When selecting the prime modulus p, a safe prime is usually used where $(p-1)/2$ is also prime. Say we select $p = 11$.

Because $(p-1)/2$ is also a prime, any value of g where $1 < g < p - 1$ will suffice; here we use $g = 2$.

Say A chooses $x = 5$ and b chooses $y = 6$.

A computes $2^5 \pmod{11} = 10$ and sends this to B.

B computes $2^6 \pmod{11} = 9$ and sends this to A.

A and B compute the shared secret $9^5 \pmod{11} = 10^6 \pmod{11} = 1$

4(b) [7 Marks]

Show how DH key exchange is subject to a man-in-the-middle attack.

Solution:
The man-in-the-middle attack with attacker I is as follows:

1. A chooses a random x such that $1 < x < p - 1$.
2. $A \rightarrow I : g^x \pmod{p}$
3. I chooses a random z such that $1 < z < p - 1$.
4. $I \rightarrow B : g^z \pmod{p}$
5. B chooses a random y such that $1 < y < p - 1$.
6. $B \rightarrow I : g^y \pmod{p}$
7. $I \rightarrow A : g^z \pmod{p}$
8. A computes $K = (g^z)^x \pmod{p}$.
9. B computes $K' = (g^z)^y \pmod{p}$.
10. I shares K with A and K' with B.

4(c) [5 Marks]

Describe in detail two ways in which the man-in-the middle attack on DH can be avoided.

Solution:
Some ways in which the man-in-the-middle attack can be avoided are as follows:

- Embedding the key exchange into an authentication protocol such as the Needham-Shroeder public key protocol.
- Both participants can digitally sign key material prior to encryption, as is done in the STS protocol.

- Both participants can make use of a shared password, as is done in the SPEKE protocol.

[End Question 4]

QUESTION 5 ***[Total marks: 20]***

5(a) [5 Marks]

Explain the difference between *entity authentication* and *message origin authentication*. Which form of authentication can be provided in a secure e-mail system? Explain your answer.

Solution:
Entity authentication is where an entity proves their identity. This is not possible with an e-mail system because it is a store-and- forward protocol and the originator of a message is not online when a message is received. Message origin authentication allows the identity of a message originator to be verified. This is possible in a secure e-mail system through the use of digital signatures.

5(b) [7 Marks]

Explain how a combination of symmetric and asymmetric ciphers can be used to implement secure e-mail. Your answer should explain the use of *message keys* and *tokens*.

Solution:
Symmetric ciphers can be used to encrypt the message body to provide confidentiality. In this context the session key is normally referred to as a message key. Asymmetric ciphers can be used to digitally sign messages to provide message origin authentication. If a recognized PKI is used, this also provides non-repudiation of origin. Asymmetric ciphers can also be use to encrypt message keys so they can be communicated confidentially to the recipients. These encrypted message keys are called tokens.

5(c) [8 Marks]

Describe PGP and how this can be used to implement a secure e-mail system.

Solution:
PGP offers the following services:

- Authentication using digital signature
- Confidentiality using message encryption
- Compression
- Email compabitility
- Segmentation

Symmetric encryption/decryption is performed using CAST-128/IDEA/3DES. Asymmetric encryption/decryption is performed using RSA/ElGamal. Digital signatures are performed using RSA/DSS.

[End Question 5]

[END OF EXAM]