

Final Exam

Solutions

Problem I

1. The major weakness of this method is the transmission of the key over an unsecured channel. Since the key can be intercepted, all subsequent communications encrypted with the key can be decrypted. Increasing the size of the key does prevent the interception of the key, therefore it does not increase the security of the method where it needs to be increased.

2.

From: andrew@example.com
To: barbara@example.com
Subject: Secret Message

Dear Barbara,

I have generated three large numbers a , g and p .

I am attaching to this e-mail the hexadecimal string of g , p and $g^a \bmod p$.

Please choose a number b and send me $g^b \bmod p$ (do not send me b).

Regards,

Andrew

From: barbara@example.com
To: andrew@example.com
Subject: Re: Secret Message

Dear Andrew,

I have received your e-mail and your numbers.

Following your request, please find attached $g^b \bmod p$.

Regards,

Andrew

From: andrew@example.com
To: barbara@example.com
Subject: Re: Secret Message

Dear Barbara,

I have received your number.

Please use $(g^a \bmod p)^b$ as the key to AES.

On my side, I'll use $(g^b \bmod p)^a$, which is equal to $(g^a \bmod p)^b$.

Regards,

Andrew

3. The downside of the solution presented in the previous question lies in the risk of a man-in-the-middle attack. Someone could intercept the communication between Andrew and Barbara and replace the numbers sent by each party with his own numbers. This attack is known as a man-in-the middle attack.

Problem II

The number AA in base 16 is equal to 10101010 in base 2, which corresponds to

$$x^7 + x^5 + x^3 + x$$

in \mathbb{F}_{256} .

First we look for the inverse of this element. Since we chose $x^8 + x^4 + x^3 + x + 1$ to be the irreducible polynomial to create \mathbb{F}_{256} from $\mathbb{Z}/2\mathbb{Z}[x]$, we need to solve

$$(x^7 + x^5 + x^3 + x)P + (x^8 + x^4 + x^3 + x + 1)Q = 1$$

This can be done by using the Euclid Algorithm.

First we compute the division of $x^8 + x^4 + x^3 + x + 1$ by $x^7 + x^5 + x^3 + x$.

$$\begin{array}{r} x \\ x^7 + x^5 + x^3 + x \overline{) x^8 + x^4 + x^3 + x + 1} \\ \underline{x^8 + x^6 + x^4 + x^2} \\ x^6 + x^3 + x^2 + x + 1 \end{array}$$

It should be noted that $-1 = 1$ in \mathbb{Z}^2 . If you are prone to sign errors, this is somewhat good news. It follows that

$$(x^8 + x^4 + x^3 + x + 1) = x(x^7 + x^5 + x^3 + x) + (x^6 + x^3 + x^2 + x + 1) \quad (1)$$

We also have

$$(x^7 + x^5 + x^3 + x) = x(x^6 + x^3 + x^2 + x + 1) + (x^5 + x^4 + x^2) \quad (2)$$

We also have

$$\begin{array}{r} x \quad +1 \\ x^5 + x^4 + x^2 \overline{) x^6 + x^3 + x^2 + x + 1} \\ \underline{x^6 + x^5 + x^3} \\ x^5 + x^2 + x + 1 \\ \underline{x^5 + x^4 + x^2} \\ x^4 + x + 1 \end{array}$$

It follows that

$$(x^6 + x^3 + x^2 + x + 1) = (x + 1)(x^5 + x^4 + x^2) + (x^4 + x + 1) \quad (3)$$

Similarly, we have

$$(x^5 + x^4 + x^2) = (x + 1)(x^4 + x + 1) + 1 \quad (4)$$

which confirms that the two polynomials we considered are coprime. From (4), we have

$$1 = (x^5 + x^4 + x^2) + (x + 1)(x^4 + x + 1)$$

From (3), we get

$$1 = (x^5 + x^4 + x^2) + (x + 1)[(x^6 + x^3 + x^2 + x + 1) + (x + 1)(x^5 + x^4 + x^2)]$$

$$1 = (x + 1)(x^6 + x^3 + x^2 + x + 1) + x^2(x^5 + x^4 + x^2)$$

From (2), we get

$$1 = (x+1)(x^6 + x^3 + x^2 + x + 1) + x^2[(x^7 + x^5 + x^3 + x) + x(x^6 + x^3 + x^2 + x + 1)]$$

$$1 = x^2(x^7 + x^5 + x^3 + x) + (x^3 + x + 1)(x^6 + x^3 + x^2 + x + 1)$$

From (1), we get

$$1 = x^2(x^7 + x^5 + x^3 + x) + (x^3 + x + 1)[(x^8 + x^4 + x^3 + x + 1) + x(x^7 + x^5 + x^3 + x)]$$

$$1 = (x^3 + x + 1)(x^8 + x^4 + x^3 + x + 1) + (x^4 + x)(x^7 + x^5 + x^3 + x)$$

It follows that the inverse of $x^7 + x^5 + x^3 + x$, in \mathbb{F}_{256} is

$$x^4 + x$$

which corresponds to

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Let us compute

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

This corresponds to 10101100 which is a binary representation of AC .

Problem III

1. This is a X509 (V3) certificate issued by Verisign to John Cagnol. This is not a self-signed certificate since the issuer and the subject have different distinguished names. The serial number is assigned uniquely to the certificate as a means to identify it without ambiguity in the revocation list.

2.

Issued to: John Cagnol (CN)
Signed by: Verisign, Class 1 ... (CN)

3.

a . Valid until Oct 8 2010

b . This one validity is a mechanism to invite the certificate owner to renew it and of course pay for it.

c . December 31st 2037, since the Y2K38 bug might trigger some problems...

4.

a . The certificate uses RSA as the primary signature algorithm, combined with the SHA-1 hash algorithm. This is identified by the signature field: sha1WithRSAEncryption.

b . This is a signed certificate. The signature made by the issuer (here Verisign) is issued to assert that the certificate is valid. This only works if the signer is trusted.

c . The ASN.1 description of a certificate is as follows. It shows that the signature is computed from the tbsCertificate part.

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue      BIT STRING
}
```

d . The SHA-1 hash function is used to compute the integer value of the tbsCertificate. The certificate is validated by computing the SHA-1 message and comparing the value with the reverse signature computed with the signature public key. If someone changes the signature or the certificate content, the signature validation algorithm will fail. Note that the key used to sign the certificate has nothing to do with the certificate public key.

5. Multiple OU fields are not a problem in a certificate. The most important part of the RDN is the common name (CN).

6.

a . This is an RSA key

b . The answer is 2048 bits

c . Yes, it is a strong key according to today's security standard

d . This an RSA public key. It can be used to encode a message that can only be read by the certificate owner who owns the private key. The RSA algorithms encrypt a message with the following formula: $E = M^e \pmod m$ where M is the message, e the RSA exponent and m the RSA modulus.

7. This certificate cannot be used in a web browser since the common name (CN) does not reference a host name.

8. This is a certificate issued by Starfield Secure Certification Authority (CN) to cagnol.com. This is not a self-signed certificate and it has nothing to do with the first one. However, its structure is similar and uses sha1WithRSAEncryption algorithm as the primary signature algorithm.

9. This certificate can be used in a web browser since the common name is cagnol.com. Note also that the extension provides an alternative name which is: www.cagnol.com

10. The concerned person is John Cagnol.