Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2016–2017, Semester: 2

Prof. G. Pelosi

September 12th, 2017 – Exam Session

Name: ..... Surname: .....

Student ID: ..... Signature: .....

Time: 2h:30'. Use of textbooks, notes, or Internet connected devices (including smartphones) is not allowed. The usage of simple calculators is allowed. Prior to turn in your paper, write your name on any additional sheet and sign it.

Question 1 [4 pts]
Consider the Transport Layer Security (TLS) protocol employing the centralized Public Key Infrastructure (PKI) authentication method.

(a) Justify which among these two choices for a ciphersuite is the best one, i.e., provides the highest overall security level in all the guaranteed properties: i) AES-256, SHA2-256, ECDSA on the standard NIST P-256 curve and ECDH over the same curve; ii) AES-192, SHA2-384, ECDSA on the P-384 curve and ECDH on the same curve.

(b) Consider the case where the server certificate is signed by a compromised CA, and assume that the root CA issuing certificates for the compromised CA is aware of this fact, and has thus revoked its certificate. Describe in detail the certificate verification process performed by a client during the TLS handshake up to the point where the server certificate is rejected, and state why it is rejected.

Solution:

(a) Choice ii) is the preferred one as it provides a consistent 192b security level, while choice i) is limited to a 128b security by both the choice of the asymmetric primitives for signing and key agreement, and the length of the digest of SHA2-256.

(b) The TLS handshake states that the server provides to the client its certificate for the client to verify in the *ServerHello* message. The client, starts the verification process checking the issuer of the server certificate, and notices that it is not a root CA. It thus proceeds checking recursively the issuers up to the point where a root CA is reached (only one step in the question at hand, since it is the root CA who issued the revocation). The client then verifies the signature of the root CA on the compromised ca certificate and finds it to be valid. However, when the client checks the revocation status of the certificate, either via OCSP, or fetching the most recent CRL, it finds out that the certificate is invalid, and thus rejects in on this base.

Question 2 [6 pts]
Alice and Bob want to use a block cipher to encrypt their communications and need to choose a mode of operation between the CTR mode and the CBC mode. Consider the following scenarios, assuming that an (active) adversary is able to intercept and change messages sent from Bob to Alice.

(a) In some messages sent by Bob, the last block is a randomly generated secret key.
Discuss if the use of the aforementioned modes of operation allows the adversary to corrupt the last block of the ciphertext without being noticed (i.e., if the adversary can change the last block so that Alice receives a message that looks good after decryption, but contains the wrong key).

(b) In some messages sent by Bob, the adversary may know the first plaintext block M_1 and may want to replace it by another block A_1 of her choice, leaving the rest of the message unchanged.
Show how the adversary can successfully deceive Alice to decrypt A_1 if CTR mode is used.
Do you think she can do the same also when the CBC mode is employed?
Would you change your answer to the previous question if the adversary is allowed to replace the ciphertext block containing the initialization value (C_0=IV)?

Solution:

(a) For both modes it is the case that the adversary can replace the last ciphertext block with another value without being noticed.
Indeed, as the adversary knows that the last block will be computed as the encryption of a randomly generated secret key value, even if she corrupts it, there is no way for the recipient to discover that.

(b) In case the CRT mode of operation is employed, the sender (Bob) will compute the first ciphertext block C_1 as $C_1{=}M_1{\oplus}\mathrm{Enc}_k(\mathtt{IV}||1)$. When the adversary intercepts this block, knowing M_1 she can easily compute $\mathrm{Enc}_k(\mathtt{IV}||1){=}M_1{\oplus}C_1$, and then replace C_1 with the encryption C_1' of another plaintext (A_1) of her choice, i.e.: $C_1'{=}A_1{\oplus}\mathrm{Enc}_k(\mathtt{IV}||1){=}A_1{\oplus}M_1{\oplus}C_1$.

In case the CBC mode of operation is employed, the decryption operation will allow the legitimate receiver (Alice) to derive the plaintext M_1 as $M_1{=}\mathrm{Dec}_k(C_1){\oplus}C_0$.
The adversary cannot change C_1, since that would also affect the decryption of C_2.
However, the adversary sees C_0 and knows M_1, thus she can compute $\mathrm{Dec}_k(C_1){=}M_1{\oplus}C_0$.
The best she can do is to try finding another value C_0' such that $A_1{=}\mathrm{Dec}_k(C_1){\oplus}C_0'$.
In case of success, as the following equalities hold: $C_0'{=}A_1{\oplus}\mathrm{Dec}_k(C_1){=}A_1{\oplus}M_1{\oplus}C_0$,
it will be easy for her to deceive Alice through replacing C_0 with C_0'.

Question 3 [6 pts]
Consider the group of points over the elliptic curve $\mathbb{E}(\mathbb{F}_{17}) : y^2 = x^3 + x$, with order $n{=}|\mathbb{E}(\mathbb{F}_{17})|{=}16$.

(a) Verify the "non-singularity" of the curve and compute the number of generators of the group.

(b) Verify that P$=(1, 6)$ generates a subgroup of order 4, then compute the coordinates of Q$=-$P and show its order.

(c) Discuss the parameter settings and the mathematical security of an elliptic curve cryptosystem employing a group with a composite order.

Solution:

(a) $4 \cdot 1^3 + 27 \cdot 0^2 \bmod 17 = 4 \neq 0 \bmod 17$. $n = 16$, Number of generators: $\varphi(n) = 8$.

(b) P$=(x_1, y_1) = (1, 6)$.
$[2]\mathrm{P} = (x_2, y_2)$,
$\lambda = (3 \cdot 1^2 + 1) \cdot (2 \cdot 6)^{-1} \equiv_{17} 3^{-1} \equiv_{17} 6$,
$x_2 \equiv_{17} \lambda^2 - 2 \cdot x_1 \equiv_{17} 6^2 - 2 \cdot 1 \equiv_{17} 0$,
$y_2 \equiv_{17} -y_1 + \lambda \cdot (x_1 - x_2) \equiv_{17} -6 + 6 \cdot (1 - 0) \equiv_{17} 0$.
$[4]\mathrm{P} = [2]([2]P) = (x_4, y_4)$,
$\lambda = (3 \cdot 0^2 + 1) \cdot (2 \cdot 0)^{-1} \equiv_{17} ...$, $[4]\mathrm{P} = (x_4, y_4) = \mathcal{O}$.

Q $= -\mathrm{P} = (1, 11)$. The order is the same of P. Denoting as $l = 4$ the order of P and as m the order of Q, we have that $[m]\mathrm{Q} = \mathcal{O} \Leftrightarrow [m](-\mathrm{P}) = [m]([l-1]\mathrm{P}) = \mathcal{O}$ thus m must be such that $[m]\mathrm{P} = O$, hence $m = l = 4$.

(c) see lectures...

Question 4 [4 pts]
Consider an ElGamal cryptosystem employing a cyclic group $(G, \cdot)$ with order $n = 43$ and generator g, and suppose Bob's private key is 10.

(a) What is Bob's public key, and what is his decryption function?
If Alice wishes to send the message $m \in G$ to Bob, and chooses a random number $l = 7$, what ciphertext does Bob receive? Check that his decryption function correctly recovers m. (All working should be expressed in terms of the "variables" g and m.)

(b) How can you define the ElGamal encryption protocol to work with the group of points of an elliptic curve?

Solution:

(a) $k_{\texttt{pub-Bob}} = (n, g, g^s) = (43, g, g^{10})$, $k_{\texttt{priv-Bob}} = (s) = (10)$.
Bob receives $c = \langle \gamma, \delta \rangle$, with $\gamma = g^l \in G$, $\delta = m \cdot (g^{10})^l \in G$, l a random element of $\mathbb{Z}_n^*$ and decrypt the message through computing
$\mathrm{Dec}_{k_{\texttt{priv-Bob}}}(c) = \gamma^{n-s} \cdot \delta \equiv m \cdot g^{-10\,l} \cdot (g^{10})^l \equiv m$.
If $l = 7$, Bob receives $c = \langle \gamma, \delta \rangle = \langle g^7, m \cdot g^{27} \rangle$.

(b) see lectures...

Question 5 [12 pts]

(a) Apply the Pollard's rho factorization method to the RSA modulus $n = p \cdot q = 391$, showing each step of the computation.

(b) Given the public exponent $e{=}3{\in}\mathbb{Z}^*_{\varphi(n)}$, show the value of the RSA private key $k_{priv}{=}(p, q, \varphi(n), d)$. Show every step of the computation.

(c) Decrypt the message $c = 222_{\mathrm{dec}} \in \mathbb{Z}_n$ (provided without any padding scheme) through applying the CRT. Describe each step of the computation. Quantify the advantage of applying the CRT compared to the execution of the non-optimized RSA decryption function.

(d) Discuss about the mathematical security of the RSA cryptosystem. What is a "good" choice for the key-length parameter of an RSA scheme?

(e) Assume to work into the Montgomery domain: $(\mathbb{Z}_N, +, \times)$, $N = 33$

- Show the definition of the Montgomery Multiplication strategy and show an high-level pseudo-code to implement the RSA decryption function employing the Montgomery arithmetics.
- Compute the Montgomery multiplication $C = A \times B \bmod N$, where $A = 24_{\text{dec}}$ and $B = 31_{\text{dec}}$ are values in the Montgomery domain. Assume a binary encoding of the operands.

Solution:

(a) ... $p = 17, q = 23$.

(b) $e{=}3{\in}\mathbb{Z}^*_{352}$, $\varphi(n) = 352$, $\varphi(352) = 160$, $d \equiv_{352} e^{159} \equiv_{352} \ldots \equiv_{352} 3^{159} \equiv_{352} 235$.
$k_{priv} = (p, q, \varphi(n), d) = (17, 23, 352, 235)$.

(c) ... applying the CRT ... $m \equiv_{391} 205$; see lectures...

(e) $C = 24_{\text{dec}} = \langle 011000 \rangle_2$ ... see lectures...