Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

July 25th, 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 a common PKI infrastructure based on X.509 certificates.

(a) You have received a certificate for `www.site-A.com` signed by rootCA-A. Recently, rootCA-B has been compromised, but the news did not reach you.
The validity of your certificate is affected by the news in any way?
Does it change anything if you still have to retrieve the certificate for `www.site-A.com`, and you do not know yet who is signing it?

(b) What is the (approximate) total size of a 100KiB non-compressed email message encrypted for ten recipients in the OpenPGP format?

(c) Consider the case of Alice willing to send an email to Bob encrypting it with OpenPGP. Alice fetches the Bob's certificate from a public-key server. She knows that Dave signed Bob's certificate but she doesn't find Dave's signature on the certificate she retrieved.
How can she be sure that the certificate is authentic?

Question 2 [**4 pts**]
Consider the case of a password hashing scheme employing SHA-256 as its compression function.

(a) Assuming that the passwords are composed of 8 random printable ASCII characters (there are 128 of them), compute the chain length and size of the rainbow table you would use, assuming that you have 64 GiB of RAM available.

(b) Compute the size of the salt, assuming it is composed of fully random bits, to prevent a Time-To-Memory-Tradeoff (TMTO) from being performed, assuming that computing 2^{128} SHA-256 hashes is unfeasible.

(c) Consider the following two password hashing strategies for an 8 printable ASCII characters password `p` an 8 B salt `s`. The notation `p[i:j]` indicates the portion of the password starting at byte `i` and ending at byte `j`, and the same goes for the salt. The || symbol denotes bitwise concatenation.

Strategy A: SHA-256(`p[0:2]||s[0:2]||p[3:5]||s[3:5]||p[6:7]||p[6:7]`)

Strategy B: SHA-256(`p[0:2]||s[0:2]`)||SHA-256(`p[3:5]||s[3:5]`)||SHA-256(`p[6:7]||p[6:7]`)

Justify which one of the choices is better, computing the effort to perform an exhaustive search for the password value given a hash in terms of the required number of SHA-256 hash computations.

Question 3 [6 pts]

The *Pohlig-Hellman Exponentiation Cipher* is a symmetric key cipher.
Its definition assumes that a prime p is publicly known, and that a plaintext message m and its corresponding ciphertext c belong to $\mathbb{Z}_p$.
The secret key of the cipher is $k=(k_{\texttt{enc}}, k_{\texttt{dec}})$, where $k_{\texttt{enc}}=e\in\mathbb{Z}^*_{\varphi(p)}$ is employed for encryption, while $k_{\texttt{dec}}=d\in\mathbb{Z}^*_{\varphi(p)}$ is employed for decryption, with $e\cdot d\equiv_{\varphi(p)}1$.
A message $m\in\mathbb{Z}_p$ is encrypted as: $c\leftarrow \text{ENC}_{k_{\texttt{enc}}}(m)=m^e \bmod p$, while the corresponding ciphertext is decrypted as: $m\leftarrow \text{DEC}_{k_{\texttt{dec}}}(c)=c^d \bmod p$.

(a) Explain how to recover the secret key given one plaintext-ciphertext pair.

(b) Prove the correctness of the cipher for every value of p and m, and state the criteria you should employ to choose the value of p.

(c) Consider the choice $p=10223\cdot 2^{31172165}+1$. Is the corresponding instance of the Pohlig-Hellman Exponentiation Cipher secure? Justify your answer.

Question 4 [6 pts]

Consider the cyclic group $G=(\mathbb{Z}^*_{19}, \cdot)$.

(a) List all subgroups of G, exhibiting at least one generator for each of them.

(b) Compute the following discrete logarithm $x \equiv \log^{\texttt{D}}_3(-1)$ applying the Pohlig-Hellman method.

Question 5 [15 pts]

(a) Describe the Pollard's $P-1$ factorization method.

(b) Consider the RSA modulus $n = p \cdot q = 253 = 11 \cdot 23$

- Given the public exponent $e=7 \in \mathbb{Z}^*_{\varphi(n)}$, show the value of the RSA private key, $k_{priv}=(p, q, \varphi(n), d)$ and specify every step of the computation.
- Apply a Square & Multiply strategy to sign the message $m=25_{\text{decimal}}$, employing a radix-4 encoding of the exponent.
- Apply the CRT to sign the message $m=25$, showing every step of the computation.

(c) Compare the asymptotic computational complexity of performing the RSA signature with the CRT to the one of computing the same signature employing a plain S&M strategy with an exponent encoded in a radix $R=2^w$.

(d) Explain the Montgomery strategy for performing modular multiplications, highlighting its advantages in implementing RSA or dlog-based primitives.

(e) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_p, +, \times)$, $p=31$, and compute the Montgomery multiplication $\widetilde{C}=\text{MonPro}(\widetilde{A}, \widetilde{B})$, where $\widetilde{A}=16_{\text{dec}}$ and $\widetilde{B}=15_{\text{dec}}$, assuming a binary encoding of the operands.