Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2017–2018, Semester: 2

Prof. G. Pelosi

July 17th, 2018 – 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 case of a per-file data-at-rest encryption, where a single block cipher key is employed for every file.

(a) From a performance standpoint, which mode of operation would you choose between CBC and CTR for encrypting/decrypting each file in the mentioned scenario?

(b) From a security standpoint, which mode of operation would you choose between CBC and CTR? (Hint: Distinguish the case where the `IV`s of two files are different from the one where they match...)

Solution:

(a) Seeking a block and decrypting it is equally efficient both using CBC and CTR. However, small modifications to a CBC encrypted file will require the re-encryption of the blocks following the modified one. This does not happen in CTR where it is possible to modify selectively only the intended block.

(b) If two files have different (unique and unpredictable) `IV`s, both the CBC and CTR modes of operation are ok. If the `IV`s of two distinct files match,

- a CBC encryption will allow to distinguish the longest common prefix between the plaintexts, checking what is the longest number of equal blocks between the ciphertexts starting from the `IV`s.
- a CRT encryption will allow to obtain the unencrypted difference (i.e., the xor) between the two plaintexts, simply computing the `xor` between the ciphertexts. This is particularly critical if one block in either one of the two files is zero-filled as the result of the difference will reveal the other block plaintext.

Question 2 [4 pts]
Consider the following two password hashing schemes:

1. Accept a seven lowercase alphabetic character password. Draw a random salt s, 32b in length, compute $h = \text{SHA-2-256}(s||\texttt{password}||s)$. Store $h||s$.

2. Accept seven lowercase alphabetic strings drawn at random from an English dictionary with 65536 terms. Compute $h = \text{SHA-2-256}(s_1||s_2||s_3||s_4||s_5||s_6||s_7)$ and store h

Argue which one of the two password schemes can be fruitfully attacked with a time to memory tradeoff such as a rainbow table. For the said scheme, compute the chain length of a rainbow table, assuming to have 16 GiB of available storage, and employing a storage strategy which has no overhead save for storing the table data (i.e., omit any storage requirement for the indexing). Considering the time to compute SHA-2-256 to be 100μs, and the time to perform a table lookup to be 1μs, compute the worst case password finding time.

Solution:
Considering the effective password space of the two schemes, taking into account the presence of the salt, we have that:

1. Scheme 1 has an effective password space of $2^{7\log_2(26)+32} \approx 2^{65}$.
2. Scheme 2 has an effective password space of $2^{7\log_2(65536)} = 2^{112}$

We thus have that the second scheme cannot be attacked via TMTO as the effort of building the rainbow tables (i.e. 2^{112} password hash computations) is not practically feasible.

For the first scheme, computing $\approx 2^{65}$ hashes is feasible. Willing to employ 16 GiB to store the rainbow table, consider the fact that an entry of the table is as large as two SHA-2-256 digests, i.e. $32 \cdot 2 = 64$B. The table will thus be able to store $\frac{2^{34}}{2^6} = 2^{32}$ chains. Each one of such chains will have to span a portion of the keyspace equal to $\frac{2^{65}}{2^{32}} = 2^{33}$ passwords, thus the chain will be 2^{33} hashes long. The worst case password finding time is given by a sequence of alternated password hashing and rainbow table lookup as long as the table itself. We thus have that the worst-case password finding time is $2^{33} \cdot 101 \cdot 10^{-16}$s which is approximately $2^{23} \cdot 101$s or 26.8 years

Question 3 [3 pts]
Considering the Tor transport anonymity protocol:

1. What is the working principle providing transport anonimity in the Tor relay network?
2. When is a malicious relay able to selectively drop the relay cells belonging to the circuit of a specific client connected to the Tor network?

Solution:

- See lectures.
- Only in case it is the entry node of the said client. Indeed, in all the other cases, the relay will only see opaque relay cells without the possibility of determining their source.

Question 4 [10 pts]

(a) Consider an instance of the Diffie-Hellmann protocol with public parameters described as follows: $G \subseteq (\mathbb{Z}^*_{73}, \cdot)$, $G = \langle g \rangle$. Compute the cardinality of the group, the number of its generators and the number of subgroups.

(b) Consider an instance of the Diffie-Hellmann protocol with public parameters described as follows: $G \subseteq (\mathbb{F}_{7^3}^*, \cdot)$, $G = \langle g \rangle$. Compute the cardinality of the group, the number of its generators and the number of subgroups.
Find the number of irreducible and primitive polynomials that can be employed to represent the field elements.
Determine if $f(x) = x^3 - x - 1 \in \mathbb{F}_7[x]$ is reducible or not.

(c) Keeping into account the Pohlig-Hellman attack, which cyclic group between $(\mathbb{Z}_{7^3}^*, \cdot)$ and $(\mathbb{F}_{7^3}^*, \cdot)$ is preferable?

Solution:

(a) $|(\mathbb{Z}_{343}^*, \cdot)| = \varphi(343) = \varphi(7^3) = 7^3 - 7^2 = 294$;
Num. of generators: $\varphi(|(\mathbb{Z}_{343}^*, \cdot)|) = \varphi(\varphi(343)) = \varphi(294) = \varphi(2 \cdot 3 \cdot 7^2) = (2^1 - 1) \cdot (3^1 - 1) \cdot (7^2 - 7) = 1 \cdot 2 \cdot 42 = 84$.
Num. of proper divisors of $|(\mathbb{Z}_{343}^*, \cdot)| = \varphi(343) = \varphi(7^3) = 294$ is equal to 10 (i.e., 2, 3, 6, 7, 14, 21, 42, 49, 98, 147); this value coincides with the number of proper subgroups of $(\mathbb{Z}_{343}^*, \cdot)$.

(b) $|(\mathbb{F}_{7^3}^*, \cdot)| = 7^3 - 1 = 342$.
Num. of generators: $\varphi(|\mathbb{F}_{7^3}^*|) = \varphi(342) = \varphi(2 \cdot 3^2 \cdot 19) = 1 \cdot 6 \cdot 18 = 108$,
Num. of proper divisors of $|(\mathbb{F}_{7^3}^*, \cdot)| = 342 = 2 \cdot 3^2 \cdot 19$ is equal to 10 (i.e., 2, 3, 6, 9, 18, 19, 38, 57, 114, 171); this value coincides with the number of proper subgroups of $(\mathbb{F}_{7^3}^*, \cdot)$.
Number of irreducible polynomials: $N_3(7) = \frac{7^3 - 7}{3} = 112$.
Number of primitive polynomials: $M_3(7) = \frac{\varphi(342)}{3} = \frac{108}{3} = 36$.
$f(x) = x^3 - x - 1 \in \mathbb{F}_7[x]$ is reducible iif $\exists\ a \in \{0, 1, 2, 3, 4, 5, 6\}$ s.t. $f(a) \equiv_7 0$ (Ruffini's Theorem).
$f(0) \equiv_7 -1$, $f(1) \equiv_7 -1$, $f(2) \equiv_7 5$, $f(3) \equiv_7 2$, $f(4) \equiv_7 -4$, $f(5) \equiv_7 0$.
The polynomial is reducible!
Indeed, $f(x) = x^3 - x - 1 = (x - 5) \cdot (x^2 + 5x + 3)$.

(c) (see lectures)...the cyclic group must have a prime cardinality (properly sized) to prevent the application of the Pohlig-Hellman attack...the factorization of the order of $(\mathbb{Z}_{7^3}^*, \cdot)$ (i.e., $|(\mathbb{Z}_{343}^*, \cdot)| = 294$) is $B = 8$-smooth, while the factorization of the order of $(\mathbb{F}_{7^3}^*, \cdot)$ (i.e., $|(\mathbb{F}_{7^3}^*, \cdot)| = 342$) is $B = 20$-smooth.
Thus, keeping into account the computational complexity of the Pohlig-Hellman attack, the latter group looks to be preferable to the former one.
Indeed, forsaking the fact that the cardinalities of the considered groups are not cryptographically significant, we can apply the formula employed to express the computational complexity of the Pohlig-Hellman attack against a generic cyclic group G with cardinality $n = \prod_{i=1}^{s} p_i^{e_i}$,
i.e.: $\mathcal{O}\left(\sum_{i=1}^{s} e_1 \cdot (\log_2 p_i + \sqrt{p_i})\right) = \mathcal{O}\left(s \cdot \max(e_1, \ldots) \cdot (\log_2 n + \sqrt{B})\right)$,
and observe the following:
for the group $(\mathbb{Z}_{343}^*, \cdot)$ we have $3 \cdot 2 \cdot (\log_2(343) + \sqrt{8}) = 6 \cdot (8.42 + 2.83) \approx 67$ bit operations, while for the group $(\mathbb{F}_{7^3}^*, \cdot)$ we have $3 \cdot 2 \cdot (\log_2(342) + \sqrt{20}) = 6 \cdot (8.41 + 4.47) \approx 77$ bit operations; which confirms the preference expressed above.

Question 5 [14 pts]

(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 851_{\text{dec}}$. Assume $f(x) = x^2 + 1 \bmod n$ as the "random-walking" function. Show every step of the computation. (As a backup alternative, apply a "trivial division" strategy).

(b) Describe the Pollard's $P - 1$ factoring algorithms, pointing out its computational complexity.

(c) Given the values $e_1 = 3 \cdot 5$, $e_2 = 5^2$ state which of them is an admissible public exponent, motivating your answer. Show the value of the corresponding RSA public and private keys $k_{\text{pub}}=(e, n)$, $k_{\text{priv}}=(p, q, \varphi(n), d)$.

(d) Sign the message $m=111_{\texttt{dec}} \in \mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

(e) Consider a schoolbook RSA cryptosystem employing the Montgomery multiplication as building block. Write down the pseudo code of both the encryption and the CRT-based decryption transformations, pointing out their asymptotic computational complexities.

(f) Consider the modulus $N = 23_{\text{dec}}$ and the value $A = 17_{\text{dec}}$. Assuming a binary encoding of the operands and the smallest possible value for the Montgomery radix R

- compute the value $\widetilde{A}$ that is the result of mapping A into the Montgomery domain;
- apply the Montgomery multiplication algorithm to compute $\widetilde{A}^2$.

Show every step of the computations.

Solution:

(a) $p = 23$, $q = 37, n = p \cdot q = 851$.

(b) see lectures ...

(c) $\varphi(n) = 792 = 2^3 \cdot 3^2 \cdot 11$, $e_2 = 25_{\text{dec}} \in \mathbb{Z}^*_{\varphi(n)}$, $d \equiv_{\varphi(n)} {e_2}^{-1} = -95 \equiv_{792} 697$, ...;

(d) $m_p \equiv_{23} 111^{697 \bmod 22} \equiv_{23} 19^{15} \equiv_{23} 20$,
$m_q \equiv_{37} 111^{697 \bmod 36} \equiv_{37} 0^{13} \equiv_{37} 0$,
$s = q \cdot (q^{-1} \bmod p) \cdot m_p \equiv_{851} 37 \cdot 5 \cdot 20 \equiv_{851} 3700 \equiv_{851} 296_{\text{dec}}$.

(e) see lectures ...

(f) $N = 23$, $R = 32$, $RR' - NN' = 1$,
$R' = R^{-1} \bmod N = 18$,
$N' = -N^{-1} \bmod R = -7 \bmod 32 = 25$, ...,
$\widetilde{A} = \texttt{MMul}(A, R^2) = A \cdot R^2 \cdot R^{-1} \bmod N = 17 \cdot 32 \equiv_{23} 15$,
$\widetilde{A}^2 = \texttt{MMul}(\widetilde{A}, \widetilde{A}) = 15 \cdot 15 \cdot 18 \bmod 23 = 2$, ... see lectures for the execution trace of the Montgomery multiplication with binary encoded operands.