Problem Set 2
Introduction to Modern Cryptography
Online Course (Winter Term 2018)

Bauhaus-Universität Weimar, Chair of Media Security
Course: Prof Dan Boneh, Stanford University, Problem Session: Nathalie Dittrich.
URL: `http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching`
Due Date: 13.01.2019, 23:59, via email to
`nathalie.jolanthe.dittrich(at)uni-weimar.de`.

Question 1 – Nonce-Based Encryption (2+2 Points)
Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a secure block cipher. You already know that CBC and CTR modes with E are secure against Chosen-Plaintext Attacks (CPA) up to the birthday bound ($2^{n/2}$ encrypted blocks) as long as the initial value (IV) is chosen uniformly at random for every encryption. In contrast, for nonce-based encryption, the user/adversary must provide a unique (not necessarily random) IV for each encryption. Explain for (a) nonce-based CTR mode *and* (b) nonce-based CBC mode *either* why they are also CPA-secure for up to $2^{n/2}$ blocks *or* show efficient attacks.

Question 2 – Collision-Resistance (1+2 Points)
Say, Alice and Bob communicate a lot with each other. Their messages are all encrypted with CBC, all under the same secret fixed key. Say Eve is a passive eavesdropper who sees all ciphertexts. We call *a collision* the event that two arbitrary blocks i and j of any two arbitrary ciphertexts C^a and C^b are equal : $C_i^a = C_j^b$, with $(i,j) \neq (a,b)$.

a) Assume such a collision occurred. Which information can Eve obtain about the relation between C_{i-1}^a, C_{j-1}^b M_i^a, and M_j^b?

b) After how many blocks (summed over all ciphertexts) will a collision occur with significant probability, according to the birthday paradox? After how many encrypted blocks in total will the probability be $\geq 1/2$?

Question 3 – Euler and Fermat (3 Points)
Recall Euler's and Fermat's Little Theorem and Euler's Totient function. Then calculate:

a) $\varphi(16)$, $\varphi(19)$, and $\varphi(22)$.

b) $5^{(5^5)} \bmod 14$ and $5^{(5^5)} \bmod 13$.

c) $2^{600000} \bmod 13$ and $2^{113451345501} \bmod 101$.

Question 4 – Naive RSA I (2+2 Points)

a) Let $n = p \cdot q$ be an RSA modulus for two secret large primes p and q. Show how one can efficiently compute p and q when n and $\varphi(n)$ are known.

b) Assume, the RSA moduli of Alice (n_A) and Bob (n_B) are different, but share a common prime factor p: $n_A = p \cdot q_A$ and $n_B = p \cdot q_B$. Show how an adversary who knows only n_A and n_B can factorize them efficiently.

Question 5 – Naive RSA II (4 Points)

Read Section 5 of [2] before solving the following task: Alice wants to share a symmetric key with Bob. She encrypts the small (64-bit) secret key K with Bob's public RSA key (n, e) by padding it with zeroes to 2048 bits (the length of n) and computes

$$C \leftarrow (0..0 \,\|\, K)^e \bmod n.$$

Thereupon, she sends C to Bob. Discuss *either* why this key exchange is secure *or* describe an efficient attack that can recover K with significant probability and far less than 2^{64} operations.

Question 6 – Naive RSA Signatures (3 Points)

Let n be Alice' RSA modulus, d her private, and e her public key. The naive RSA signature scheme is defined as

$$\text{Sign}_{n,d}(m) := m^d \bmod n, \qquad \text{Verify}_{n,e}(s, m) := \begin{cases} \text{true} & \text{if } s^e \bmod n = m, \\ \text{false} & \text{otherwise.} \end{cases}$$

Assume, Eve sees two valid distinct message-signature pairs (m_1, s_1) and (m_2, s_2), where $s_i = Sign_{n,d}(m_i)$. Show how an adversary that does not know d can forge a third valid signature from this information.

Question 7 – RSA Padding Oracle (2+1 Points)

Alice wants to send a 256-bit AES key k, RSA-encrypted with a modulus n to Bob. She proposes the following simple encryption algorithm: k is used at the least significant 256 bits, and the higher bits are simply filled up with zero bits:

$$c = (0 \ldots 0 \,\|\, k)^e \bmod n$$

a) Assume Bob's server is an oracle that decrypts an incoming message and first checks if the 0-bit padding is correct. If it is incorrect, then the server outputs an error message. Show how an adversary Eve can use this information to recover at least one bit of k from an eavesdropped ciphertext c.

b) How would you fix the decryption algorithm to not allow such attacks?

Question 8 – ElGamal Encryption (2+3 Points)
Repeat autonomously the definitions of group, cyclic group, generator, and group order. We denote $X \twoheadleftarrow \mathcal{X}$ to mean that X was chosen uniformly at random from a set $\mathcal{X}$.

Let $\mathbb{Z}_p^*$ be a cyclic group for some prime p. Let g be a generator in $\mathbb{Z}_p^*$. The secret key of Bob is a uniformly at random chosen value $a \twoheadleftarrow \mathbb{Z}_p^*$. His public key is (g, p, A) with $A = g^a \bmod p$. With the ElGamal encryption system, Alice encrypts a message M as follows:

$$C_1 \leftarrow g^b \bmod p, \qquad C_2 \leftarrow M \cdot A^b \bmod p.$$

Alice sends the ciphertext $C = (C_1, C_2)$ to Bob.

a) Describe how Bob can decrypt the ciphertext to obtain the original message M.

b) Assume, Alice sends a second ciphertext $C' = (C_1', C_2')$ to Bob which was created with the same b as the first ciphertext C. Show or disprove: if Eve knows the plaintext M' for the second plaintext, she can efficiently compute the message M for the first ciphertext.

Question 9 – Diffie-Hellman Key Exchange (2+2+2 Points)
Alice and Bob want to exchange keys with the Diffie-Hellman protocol. They agree on a large prime p and a generator $g \in \mathbb{Z}_p^*$. Alice chooses a secret $a \twoheadleftarrow \mathbb{Z}_p^*$ and Bob a secret $b \twoheadleftarrow \mathbb{Z}_p^*$ both uniformly at random. Alice computes $A \leftarrow g^a \bmod p$ and sends it to Bob. Bob computes $B \leftarrow g^b \bmod p$ and sends it to Alice.

a) Show how Alice and Bob compute their common key K.

b) In general, would the choice of $g = p - 1$ be a good idea? Explain briefly why/why not.

c) Assume that $p - 1 = m \cdot q$ for a small m and q also a large prime. Further, assume that Alice accidentally chooses $a = q$ as her secret exponent. Eve is an adversary that sees only the values A and B by eavesdropping. How many keys would Eve have to test to find K and why?

Question 10 – Key Lengths (2 Points)
Assume that Alice is given four TLS options from her browser for securing the connection to her bank. Which of the following ⟨cipher⟩-⟨key length⟩-⟨mode⟩, and size for RSA primes provides theoretically the highest effective security and why?

- 3DES-CBC with 4096-bit primes for RSA.
- AES-128-CBC with 3072-bit primes for RSA.
- AES-256-ECB with 2048-bit primes for RSA.
- AES-256-CBC with 1024-bit primes for RSA.

References

[1] Mihir Bellare and Chanathip Namprempre: "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm". Advances in Cryptology—ASIACRYPT 2000. Springer Berlin Heidelberg, 2000. pp. 531-545.

[2] Dan Boneh, Antoine Joux, and Phong Q. Nguyen: "Why Textbook ElGamal and RSA Encryption Are Insecure", in Proceedings of ASIACRYPT'2000.

[3] Chanathip Namprempre, Phillip Rogaway, and Thomas Shrimpton: "Reconsidering generic composition". Advances in Cryptology–EUROCRYPT 2014. Springer Berlin Heidelberg, 2014. pp. 257-274.

[4] Phillip Rogaway: "Authenticated-encryption with associated-data". In: Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002. pp. 98-107.