

Problem Set 2
Introduction to Modern Cryptography
Online Course (Summer Term 2017)

Bauhaus-Universität Weimar, Chair of Media Security

Course: Prof Dan Boneh, Stanford University, Problem Session: Eik List, Jakob Wenzel.

URL: <http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching>

Due Date: 14.07.2017, 1:30 PM, via email to [eik.list\(at\)uni-weimar.de](mailto:eik.list(at)uni-weimar.de).

Question 1 – Nonce-Based Encryption (2+2 Points)

Let $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ 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 – Generic Composition (4 Points)

Let $MAC : \{0, 1\}^k \times \{0, 1\}^* \rightarrow \{0, 1\}^{n-1}$ be a SUF-CMA-secure MAC which produces $(n-1)$ -bit authentication tags. Let $MAC'_K(M) := MAC_K(M) \parallel \text{LSB}(M)$ append the least significant bit of M to the tag. Clearly, MAC' is at least as SUF-CMA-secure as MAC .

Alice uses MAC' to construct an AE scheme from the composition of $(MAC'_{K_1}, \text{CTR}_{K_2})$ with independent secret keys K_1, K_2 , where the output of MAC' is used as initial value for a counter-mode encryption. You can assume that CTR mode uses a secure block cipher $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ internally. Given some message M , the construction computes

$$IV = MAC'_{K_1}(M) \quad \text{and} \quad C = \text{CTR}_{K_2}(IV, M),$$

and outputs (IV, C) as authenticated ciphertext. AE security means Ciphertext Integrity (CI) plus chosen-plaintext privacy (CPA). Explain briefly why this composition provides AE security *or* show an efficient attack against either its ciphertext integrity or its privacy.

Note: The following works provide deeper insights into Authenticated Encryption: [1, 3, 4].

Question 3 – Deterministic Authenticated Encryption (2 Points)

For which scenario(s) is it sensible to use deterministic instead of nonce-based authenticated encryption? Explain your answers briefly.

- When the associated data is constant.
- When the messages are cryptographic keys.
- When the messages are very small and are likely to repeat.
- When messages possess a high entropy and are highly unlikely to repeat.

Question 4 – Tweakable Block Ciphers (2+2+2 Points)

Let $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a secure n -bit block cipher. Imagine, Alice wants to transform it into a secure tweakable block cipher $\tilde{E} : \{0, 1\}^k \times \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ that takes an additional n -bit tweak T . For each of the following constructions, show *either* why it is secure against chosen-ciphertext adversaries *or* show an efficient attack.

- a) $E_K(T, M) := E_K(M_i \oplus T) \oplus T$.
- b) $E_K(T, M) := E_K(M_i \oplus T')$, where $T' \leftarrow E_K(T)$.
- c) $E_K(T, M) := E_K(M_i \oplus T') \oplus T'$, where $T' \leftarrow E_K(T)$.

Question 5 – 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 6 – 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

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

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 7 – 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

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

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

Question 8 – ElGamal Encryption (2+3 Points)

Repeat autonomously the definitions of group, cyclic group, generator, and group order. We denote $X \leftarrow \mathcal{X}$ 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 $a \leftarrow \mathbb{Z}_p^*$. 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:

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

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

- Describe how Bob can decrypt the ciphertext to obtain the original message M .
- 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 $a \leftarrow \mathbb{Z}_p^*$ and Bob a secret $b \leftarrow \mathbb{Z}_p^*$ 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.

- Show how Alice and Bob compute their common key K .
- In general, would the choice of $g = p - 1$ be a good idea? Explain briefly why/why not.
- 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 Namprempe: “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 Namprempe, 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.