Applied Cryptography

Symmetric Cryptography, Assignment 5, Wednesday, May 25, 2022

Remarks:

- Hand in your answers through Brightspace.
- Hand in format: PDF. Either hand-written and scanned in PDF, or typeset and converted to PDF. Please, **do not** submit photos, Word files, LaTeX source files, or similar.
- Assure that the name of **each** group member is **in** the document (not just in the file name).

Deadline: Wednesday, June 8, 23.59

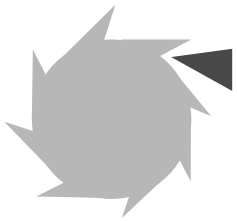
Goals: After completing these exercises you should have understanding in some techniques used in secure communication, and their limitations.

1. **(20 points)** In the lecture of May 18th, Sofia talked (a.o.) about secure communication, and the role of forward and backward security in secure communication. This question is about how the Signal protocol achieves these properties. We start with a warm up.

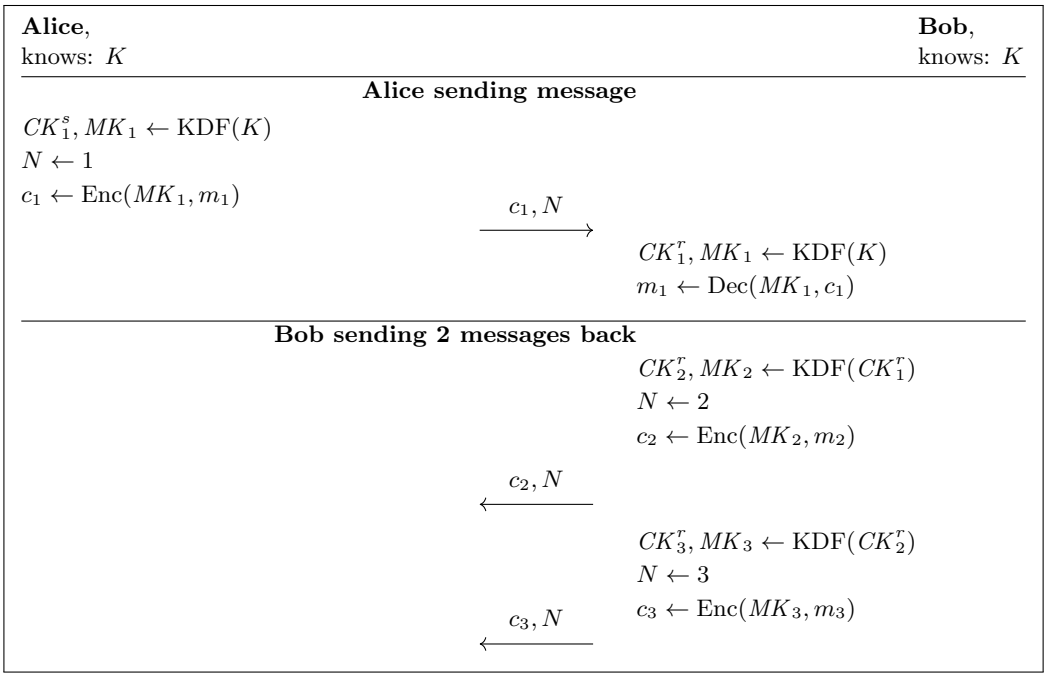
   (a) What is forward secrecy, and what is backward secrecy?

   (b) Under which condition does a Diffie-Hellman key exchange provide forward secrecy?

   The Signal protocol (`https://signal.org/docs/`) uses the so-called Double Ratchet algorithm (`https://signal.org/docs/specifications/doubleratchet/`), whose main goal is to provide forward secrecy. The name comes from a mechanical device "ratchet" that performs circular movement only in one direction. Similarly to this device, the Double Ratchet algorithm does not allow going back in a chain of derived keys.

   We start first with a single ratchet protocol. Assume Alice and Bob already share a secret key K, and use this to derive chain keys CK and message keys MK, leading to the following naive protocol to send encrypted messages. Here, KDF is a key-derivation function, Enc an encryption algorithm and Dec the associated decryption algorithm.



(c) Does this provide forward secrecy when an MK_i is leaked? What about backward secrecy?

(d) Assume leakage of CK_i at a certain moment in time. What can an attacker do with CK_i?

(e) Assume Alice and Bob have a lively conversation using the above protocol. What might go wrong with the counter N?

Considering the vulnerabilities of the naive protocol, let's explore how the double ratchet improves security. The following protocol describes a simplified view of the Double Ratchet algorithm as used in the Signal protocol. Capital letters A_i and B_i indicate public keys for Diffie-Hellman, with corresponding private keys a_i and b_i.

Alice, knows: K, B_0		**Bob**, knows: K, b_0
Alice sending message		
$a_0 \xleftarrow{\$} \mathbb{Z}_q, A_0 \leftarrow g^{a_0} \pmod p$ $SS_0 = B_0^{a_0} \pmod p$ $RK_0, CK_0^s \leftarrow \text{KDF}(K, SS_0)$ $CK_1^s, MK_1 \leftarrow \text{KDF}(CK_0^s)$ $N \leftarrow 1$ $c_1 \leftarrow \text{Enc}(MK_1, m_1)$	$\xrightarrow{c_1, N, A_0}$	$SS'_0 \leftarrow A_0^{b_0} \pmod p$ $RK_0, CK_0^r \leftarrow \text{KDF}(K, SS'_0)$ $CK_1^r, MK_1 \leftarrow \text{KDF}(CK_0^r)$ $m_1 \leftarrow \text{Dec}(MK_1, c_1)$
Bob sending 2 messages back		
		$b_1 \xleftarrow{\$} \mathbb{Z}_q, B_1 \leftarrow g^{b_1} \pmod p$ $SS_1 \leftarrow A_0^{b_1} \pmod p$ $RK_1, CK_0^r \leftarrow \text{KDF}(RK_0, SS_1)$ $CK_1^r, MK_1 \leftarrow \text{KDF}(CK_0^r)$ $N \leftarrow 1$ $c_2 \leftarrow \text{Enc}(MK_1, m_2)$
	$\xleftarrow{c_2, N, B_1}$	
		$CK_2^r, MK_2 \leftarrow \text{KDF}(CK_1^r)$ $N \leftarrow 2$ $c_3 \leftarrow \text{Enc}(MK_2, m_3)$
	$\xleftarrow{c_3, N, B_1}$	

(f) Explain the steps Alice performs to decrypt the messages. What is the role of RK_i, CK_i and MK_i in these messages?

(g) Describe, informally, what steps Alice needs to perform to send a message back to Bob.

(h) Explain what an attacker learns from the leakage of: i) RK_i, ii) CK_i, iii) MK_i.

(i) Identify the first ratchet from the naive protocol. What is the second ratchet?

(j) If, instead of using $RK_i, CK_0 \leftarrow \text{KDF}(RK_{i-1}, SS_j)$ we used $RK_i, MK_1 \leftarrow \text{KDF}(RK_{i-1}, SS_j)$, and we skip the step $CK_1, MK_1 \leftarrow \text{KDF}(CK_0)$. To encrypt a second message, we would simply compute $MK_2 \leftarrow \text{KDF}(MK_1)$. Is this less secure? What do we lose?

2. **(15 points)** In the lecture of May 25th, Peter talked (a.o.) about the Noise framework and the WireGuard protocol. The first part of this question is about certain symmetric cryptographic aspects within Noise. Refer to `http://www.noiseprotocol.org` for background study.

   (a) One authenticated encryption algorithm supported by Noise is AES-GCM. What is the official nonce size (in bits) of AES-GCM?

   (b) What is the effective nonce size (in bits) of AES-GCM as used in Noise?

   (c) Does the difference in official nonce size and actual nonce size sacrifice the *security* of the scheme? Explain your answer.

   The second part of this question is about certain symmetric cryptographic aspects within WireGuard. Refer to `https://www.wireguard.com/protocol` for background study.

   (d) What is the cryptographic hash function used in WireGuard?

   (e) WireGuard uses the HKDF mode, which, as you learned in the symmetric crypto part of the course, is heavily based on the HMAC mode. As a matter of fact, WireGuard uses standalone HMAC as well. What is the exact output size (in bits) and what is the maximal key size (in bits) for the specific HMAC construction in WireGuard?

   (f) Describe a way in which you think you can improve the way WireGuard uses the hash function you mentioned in (d). Explain your answer. [Hint: you may have to do a quick literature study to answer this question.]

   (g) What cryptographic security property on cryptographic hash functions can you use to justify your suggestion of (f). Explain your answer informally.

3. **(15 points)** In the lecture of June 1st, Thom will talk (a.o.) about TLS. This question is about an attack related to this topic, namely Bleichenbacher's attack. For this question, read the following paper: `http://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf`.

   (a) Describe the RSA PKCS#1 v1.5 padding.

   (b) What is the high level idea of the Bleichenbacher's attack?

   (c) Explain in detail the blinding step of the attack?

   (d) What can the attacker learn after obtaining one positive oracle answer?

   (e) What is the probability of obtaining one positive oracle answer?

   (f) Describe how to make a Bleichenbacher oracle for TLS. Write down a diagram that clearly indicates the oracle.

   (g) Do a literature survey and find 3 subsequent attacks based on the Bleichenbacher's attack. Write 2–3 sentences describing each of them. Don't forget to provide references.