The art of cryptography, summer 2016

MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Monday, 23 May 2016, 11:59

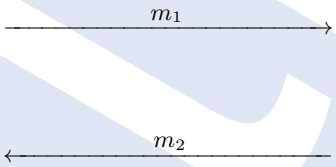
Exercise 5.1 (RSA key exchange). (10 points)

Consider the following randomized variant of the RSA key exchange:

Protocol. RSA key exchange.

Input: Security parameter κ, own identity id.

1. Bob chooses a key pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{RSA.keygen}(1^\kappa)$ and puts $m_1 \leftarrow (\mathsf{id}, \mathsf{pk})$.
2. Alice parses m_1 to obtain Bob's public key pk, generates a key $k \leftarrow \mathrm{AE.keygen}(1^\kappa)$, a random bit string $r \xleftarrow{\$} \{0,1\}^\kappa$ and encrypts this $m_2 \leftarrow \mathrm{RSA.enc}_{\mathsf{pk}}(\mathsf{pad}(\mathsf{id}, r, k))$.
   Accept, noting shared key k.
3. Bob decrypts m_2, removes the padding, parses, verifies the other identifier and extracts k.
   Accept, noting shared key k.



Mind that the input to the protocol instances is never under control of the attacker. Assume that RSA is (t, ε)-OW-POA-secure.

Discuss when this is (t', ε')-KE1-secure. Prove your findings. 10

Exercise 5.2 (Zero-Knowledge). (0+10 points)

Read Quisquater, Quisquater, Quisquater, Quisquater, Guillou, Guillou, Guillou, Guillou, Guillou, Guillou & Berson (1989) to one of your children. Alternatively take one of your fellow students.

(i) Write down the protocol in a form appropriate for computer science students rather than for children. +4

(ii) Prove for this protocol the following three properties: +6

- If the prover's claim is true, the verification returns true — always.
- If the prover's claim is false, the verification fails — with high probability.
- The verifier does not learn anything about the private information.

Exercise 5.3 (Key exchange threats). (9 points)

Consider the following protocols for establishing shared keys. We are about to discuss some aspects of security in an informal way.

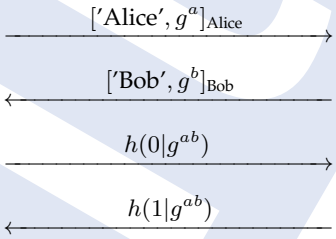
Assume there is an infrastructure such that Alice and Bob have access to any party's true public key.

For ease of notation, $[m]_{\text{Alice}}$ denotes the pair consisting of the message m and a valid public-key signature of m produced by Alice. Similarly $\{m\}_K$ shall denote the message m symmetrically authenticated and encrypted by K.

For Protocol 2 and Protocol 4 let $\pi = (G, g, q)$ be group parameters. We assume that the discrete logarithm problem relative π is suitable hard. Let h be a collision resistant hash function. For Protocol 4 Alice has a secret passphrase a and her public key is $A = g^{h(a|s)}$, where s is a random number (the "salt").

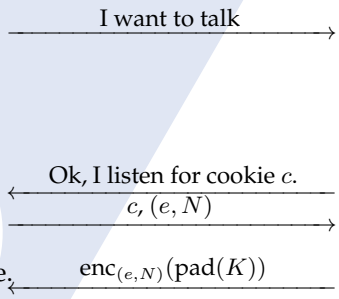
Protocol 2.

1. Alice chooses $a \in \mathbb{N}_{<\#G}$, computes g^a and signs $[\text{'Alice'}, g^a]$.
2. Bob chooses $b \in \mathbb{N}_{<\#G}$, computes g^b and signs $[\text{'Bob'}, g^b]$.
3. Alice verifies the incoming message and computes $(g^b)^a = g^{ab}$ and a hash.
4. Bob verifies the incoming message and computes $(g^a)^b = g^{ab}$ and a hash.



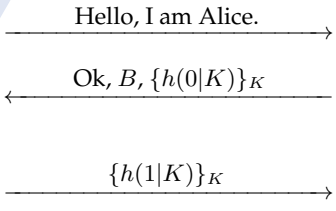
Protocol 3.

1. Alice wants to talk.
2. Bob agrees and chooses a cookie c, which is a suitably random number, for example, the hash value of Alice's IP address and some fixed secret of Bob. (It's nice if the number is deterministically determined!)
3. Alice computes RSA keys (N, e) and (N, d).
4. Bob chooses a 128-bit number K, encrypts K with Alice's RSA key (N, e) with a secure padding scheme.



Protocol 4.

1. Alice wants to talk.
2. Bob chooses $b \in \mathbb{N}_{<d}$ and computes $B = g^b$, $K = A^b$, and $h(K)$.
3. Alice computes $K = B^{h(a|s)}$, decrypts the last message and checks whether she computes the same values $h(0|K)$.
4. Bob checks whether he computes the same value $h(1|K)$.



Consider each protocol in the following questions. Be brief, but don't forget the essential arguments.

(i) *Person in the middle*: Peter puts himself in the middle. What happens? 3

(ii) *Perfect Forward Security*: Next, suppose that the Beagle Boys intercepted the conversation between Alice and Bob. Then after the conversation is terminated the Beagle Boys take over Alice' and Bob's entire equipment including their secret keys. Will they be able to read what Alice and Bob told each other? 3

(iii) *Live Partner Reassurance*: Raoul likes repetitions and so after listening to a conversation, he calls Bob (or is called by Alice) with replayed messages from the overheard talk making him (her) think she (he) is Alice (Bob). Examine the given protocols under this attack. 3

References

JEAN-JACQUES QUISQUATER, MYRIAM QUISQUATER, MURIEL QUISQUATER, MICHAËL QUISQUATER, LOUIS GUILLOU, MARIE ANNICK GUILLOU, GAÏD GUILLOU, ANNA GUILLOU, GWENDOLÉ GUILLOU, SOAZIG GUILLOU & TOM BERSON (1989). How to Explain Zero-Knowlegde Protocols to Your Children. In *Advances in Cryptology: Proceedings of CRYPTO 1989*, Santa Barbara, CA, number 435 in Lecture Notes in Computer Science, 628–631. Springer-Verlag. ISSN 0302-9743. URL `http://dx.doi.org/10.1007/0-387-34805-0_60`.