

Security on the Internet, summer 2006

MICHAEL NÜSKEN

6. Exercise sheet

Hand in solutions on Tuesday, 27th of June, at the b-it info desk. Deadline for any completely signed(!) electronic solution is the same Tuesday, 23:59.

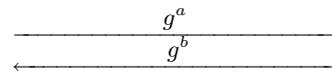
Exercise 6.1 (Key exchange threats).

(15 points)

We have considered the Diffie-Hellman key exchange: Given a group G consisting of powers of a generator g , so $G = \{1, g, g^2, \dots, g^{\#G-1}\}$ such that the discrete log problem is difficult, ie. given $h \in G$ there is no efficient (ie. randomized polynomial time) algorithm to determine i with $h = g^i$. To fix a shared secret key, Alice sends g^a and Bob sends g^b . Then both can compute the shared key g^{ab} .

Protocol 6.2. Diffie-Hellman key exchange.

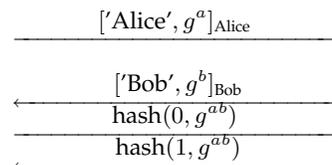
1. Alice chooses $a \in \mathbb{N}_{<\#G}$ and computes g^a .
2. Bob chooses $b \in \mathbb{N}_{<\#G}$ and computes g^b .
3. Alice computes $(g^b)^a = g^{ab}$.
4. Bob computes $(g^a)^b = g^{ab}$.



Now both can use g^{ab} to derive common secrets for the subsequent message exchanges. What if Wilma puts herself in the middle? She will have a common secret g^{aw} with Alice and a common secret g^{wb} with Bob, and as long as she continues to pass all messages on, neither Bob nor Alice will notice anything apart possibly from a slightly slower connection. So we modify this.

Protocol 6.3. Signed and acknowledged Diffie-Hellman key exchange.

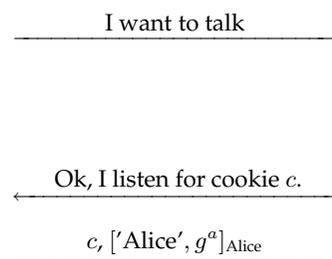
1. Alice chooses $a \in \mathbb{N}_{<\#G}$, computes g^a and signs $['Alice', g^a]$.
2. Bob chooses $b \in \mathbb{N}_{<\#G}$, computes g^b and signs $['Bob', g^b]$.
3. Alice computes $(g^b)^a = g^{ab}$ and a hash.
4. Bob computes $(g^a)^b = g^{ab}$ and a hash.



Sorry, we forgot to be polite. We should first say Hello, shouldn't we?

Protocol 6.4. Polite Diffie-Hellman key exchange with a cookie.

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 her IP address and some fixed secret of Bob. (It's nice if the number is deterministically determined!)
3. Alice chooses $a \in \mathbb{N}_{<\#G}$, computes g^a and signs $['Alice', g^a]$.



4. Bob chooses $b \in \mathbb{N}_{<\#G}$, computes g^b and signs $[\text{'Bob'}, g^b]$.
5. Bob computes $(g^a)^b = g^{ab}$ and a hash.
6. Alice computes $(g^b)^a = g^{ab}$ and a hash.

$$\begin{array}{c} \xrightarrow{[\text{'Bob'}, g^b]_{\text{Bob}}, \text{hash}(1, g^{ab})} \\ \xleftarrow{\text{hash}(0, g^{ab})} \end{array}$$

Here is a further polite variant.

Protocol 6.5. Modified Diffie-Hellman key exchange.

1. Alice chooses $a \in \mathbb{N}_{<\#G}$, computes g^a .
2. Bob chooses $b \in \mathbb{N}_{<\#G}$, computes g^b .
3. Alice computes $(g^b)^a = g^{ab}$ and uses it to encrypt her name and a signature to her share g^a .
4. Bob computes $(g^a)^b = g^{ab}$ and uses it to encrypt his name and a signature to his share g^b .

$$\begin{array}{c} \xrightarrow{\text{I want to talk, } g^a.} \\ \xleftarrow{\text{Ok, } g^b.} \\ \xrightarrow{E_{g^{ab}}(\text{'Alice'}, [g^a]_{\text{Alice}})} \\ \xleftarrow{E_{g^{ab}}(\text{'Bob'}, [g^b]_{\text{Bob}})} \end{array}$$

Consider each of the above protocols in the following questions. (Be brief, but don't forget the essential arguments.)

- 2 (i) *Woman in the middle*: Try to put Wilma in the middle. What happens?
- 2 (ii) *Mutual authentication*: Examine which of the given protocols ensure that Alice's partner is Bob.
- 2 (iii) *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's and Bob's entire equipment including their secret keys. Will they be able to read what Alice and Bob told each other?
- 2 (iv) *Denial of Service*: Daniel is a weird person that only wants to prevent say Bobs' computer to do good work. So he floods Bob with tons of requests. For each of these requests Bob's computer is forced to compute and send an answer. Consider vaguely the effort which Daniel and Bob have to spend for their first messages and vote for the 'best' protocol.
- 2 (v) *Endpoint Identifier Hiding*: Eve does not want to be spotted, so she only listens on the conversation. If she can detect who the partners are, this is already valuable information for her. Which protocols hide the identity of Alice and/or Bob?
- 2 (vi) *Live Partner Reassurance*: Romeo likes repetitions and so after listening to a conversation, he calls Bob with replayed messages from the overheard talk making him think he is Alice. (Imagine this could be successfully done when you log in to your home banking account!) Examine the given protocols under this attack.
- 3 (vii) Devise a protocol that Romeo cannot trick. (Do not forget to argue!)
- +0 (viii*) Devise a protocol that is not vulnerable to any of these attacks.