

# HW # 2

## Solution

- (5 points) Anderson claims in the paper *Why Cryptosystems Fail* that implementations of RSA should use at least a 500-bit key. Considering that this paper is about 10 years old, which key length should be chosen today for a reasonable level of security. Give a reason for your answer (Hint: look at RSA Challenge).

The last RSA Challenge that was solved had a 640-bit key. Hence, a 1024-bit key would provide a reasonable level of security today.

- (8 points) In this problem we use the DES block cipher with 64-bit input  $x$ , 64-bit output  $y$ , and 56-bit key  $k$ . We use it to construct a message authentication code MAC.

- Draw the diagram on how to build a MAC using the DES block cipher. And show the size of the output of this MAC.

See viewgraph 34 of lecture 3. Just substitute “Secret-key cipher” with DES.

- Now we use this MAC to generate authentication codes and we keep the key constant. After how many random inputs do we have a probability of  $\epsilon = 0.5$  for a collision? After how many random inputs do we have a probability of  $\epsilon = 0.2$  for a collision?

$$\text{Birthday Attack : } k \approx \sqrt{2n \cdot \ln \left( \frac{1}{1 - \epsilon} \right)}$$

Here  $n$  is the output space of the MAC or hash function, in this case  $2^{64}$  i.e. 64-bit.

$n$	$\epsilon = 0.5$	$\epsilon = 0.2$
$2^{64}$	$5.06 \cdot 10^9$	$2.87 \cdot 10^9$

Number of messages after which the probability for collision is  $\epsilon$ .

- (15 points) In this problem we will compare the security services which are provided by digital signatures (DS) and message authentication codes (MAC). We assume that Oscar is able to observe all messages send from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The signature  $sign(x)$  is computed with a DS or a MAC algorithm, respectively.

- (Message integrity) Alice sends a message  $x$ =“Transfer \$1000 to Mark” in the clear and also sends  $sign(x)$  to Bob. Oscar intercepts the message and replaces “Mark” with “Oscar”. Will Bob detect this?

Will be detected with both (i) DS and (ii) MAC.

- (b) (Replay) Alice sends a message  $x = \text{"Transfer \$1000 to Oscar"}$  in the clear and also sends  $sign(x)$  to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?  
 Won't be detected by either (Remark: use timestamps).
- (c) (Sender Authentication with cheating 3rd party) Oscar claims that he sent some message  $x$  with a valid  $sign(x)$  to Bob but Alice claims the same. Can Bob clear the question in either case?
- (i) DS: Bob simply has to verify the message with the public key from both. Obviously, only Alice's public key results in a successful verification.
- (ii) MAC: Bob has to challenge both, Oscar and Bob, to reveal their secret key to him (which he knows anyway). Only Bob can do that.
- (d) (Authentication with Bob cheating) Bob claims that he received a message  $x$  with a valid signature  $sign(x)$  from Alice e.g. "Transfer \$1000 from Alice to Bob" but Alice claims she has never sent it. Can Alice clear this question in either case?
- (i) DS: Alice has to force Bob to prove his claim by sending her a copy of the message in question with the signature. Then Alice can show that message and signature can be verified with Bob's public key  $\Rightarrow$  Bob must have generated the message.
- (ii) MAC: No, Bob can claim that Alice generated this message.
- (e) (Authentication with Alice cheating) Alice produces the message "Transfer \$100.000 from Bob to Oscar's account" and appends it with a valid signature  $sign(x)$ . She then claims that she received this message from Bob. Can Bob prove that he could not have signed this message? Hint: Oscar is Alice's little brother.
- (i) DS: Alice can not generate  $x$  which can be verified with Bob's public key. (II) MAC: No, Bob can NOT prove that he did not generate the message.