Cryptography and computer security WPPT, M.Kutyłowski, 30.11.2011

Name: .....
index number: ..... pseudonym: .....

Provide your answers on the question sheet. The answer should concern the key issues and should contain crucial arguments supporting your claims. You may answer in English, Polish. You may use any written material but no electronic devices. For each question you may get 3 points. Your results will be available in WWW in a few days, provided that you declare your pseudonym.

---

1. (for preparation) a) If we wish to test if a is a square root module a prime number p we compute $a^{(p-1)/2} \bmod p$. Recover details of such a test (do not google it!) and prove that it really works.

b) The following method is used to compute a square root r of a number a modulo a prime number p:

$$r := a^{(p+1)/4} \bmod p$$

Show that it really works provided that some conditions are fulfilled.

2. (for preparation) Kubuś i Prosiaczek boją się, że Krzyś podsłuchuje ich komunikację. Kupili więc software, który używa kluczy sesyjnych zrobionych za pomocą algorytmu DH. Niestety nie wiedzą, że software został napisany przez Krzysia. Ten zaś użył zamiast algorytmu DH:

Kubuś		Prosiaczek
choose a at random, $z_1 = g^a$		choose b at random, $z_2 = g^b$
	$\xrightarrow{z_1}$	
	$\xleftarrow{z_2}$	
$k := z_2^a$		$k := z_1^b$

jego następującej modyfikacji (p oznacza jakąś liczbę wybraną arbitralnie przez Krzysia, zaś q oznacza rząd grupy cyklicznej, w której realizowany jest protokół DH):

Kubuś		Prosiaczek
take the previous a , do $a := a \cdot 2p \bmod q$, $z_1 := g^a$		take the previous a, do $b := b \cdot p^{-1} \bmod q$, $z_2 := g^b$
	$\xrightarrow{z_1}$	
	$\xleftarrow{z_2}$	
$k := z_2^a$		$k := z_1^b$

a) W jaki sposób pozwala to Krzysiowi podsłuchiwać Kubusia i Prosiaczka?

b) Kubuś spostrzegł się, że Krzyś za dużo wie, i poszedł do Sowy po radę. Sowa widziała jednak notatki Krzysia i wie, że Krzyś nieświadomie używał grupy z odwzorowaniem dwuliniowym. I wymamrotała *sprafcie najpierf odwzorowaniem dwuliniowym*. Co Kubuś ma zrobić by odkryć taką modyfikację jak opisana nie zaglądając do kodu programu Krzysia??

3. (for preparation) Nastepujący protokół Schnorra pokazuje, że Kłapouchy zna dyskretny logarytm z $y = g^x$ (w grupie rzędu q). Pokazać że jest to protokół typu Zero Knowledge Proof. Oto opis pojedynczej rundy protokołu, gdzie oszust zostałby przyłapany z prawdopodobieństwem $\frac{1}{2}$:

Kubuś, public key $y = g^x$, secret x		Verifier checking that Kubuś has discrete logarithm of y
choose r at random, $t := g^r$		
	$\xrightarrow{t}$	
		choose c at random
	$\xleftarrow{c}$	
$s := r + xc \bmod q$		
	$\xrightarrow{s}$	
		check if $g^s = t \cdot y^c$

4. (for preparation) Rozważmy protokół uwierzytelniania przy pomocy wspólnego klucza symetrycznego k opisany poniżej. Porównać protokół ten z protokołem PACE pod względem odporności na atak przez obserwatora mającego dostęp do komunikatów wymienianych w protokole.

Kubuś, posiada klucz π		Prosiaczek, posiada klucz π
choose a at random	$\xrightarrow{a}$	
		choose b at random, $z := E_\pi(a, b)$
	$\xleftarrow{z}$	
$h := D_\pi(z)$, $h = (h_1, h_2)$		
if $h_1 \neq a$, then abort		
$z' := E_\pi(h_2, a)$	$\xrightarrow{z'}$	
		if $D_\pi(z') \neq (b, a)$, then abort

Dla przypomnienia PACE bez pewnych szczegółów (M jest pewnym odwzorowaniem na elementy grupy, załóżmy że nie daje to żadnych punktów zaczepienia do ataku):

karta z hasłem π		czytnik z π podanym przez posiadacza karty
choose s at random		
$z := E_{H(\pi)}(s)$	$\xrightarrow{z}$	
		$s := D_{H(\pi)}(z)$
$\hat{g} = M(s)$		$\hat{g} = M(s)$
run DH for generator $\hat{g}$		