COMP547B Homework set #5

Due Friday April 13th, 2018, 23:59:59

Exercises (from Katz and Lindell's book)

11.6 Consider the following public-key encryption scheme. The public key is $(\mathbb{G}, q, g, h)$ and the private key is x, generated exactly as in the El Gamal encryption scheme. In order to encrypt a bit b, the sender does the following:

[5%] (a) If $b = 0$ then choose a uniform $y \in \mathbb{Z}_q$ and compute $c_1 := g^y$ and $c_2 := h^y$. The ciphertext is $\langle c_1, c_2 \rangle$.

[5%] (b) If $b = 1$ then choose independent uniform $y, z \in \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := g^z$, and set the ciphertext equal to $\langle c_1, c_2 \rangle$.

Show that it is possible to decrypt efficiently given knowledge of x. Prove that this encryption scheme is CPA-secure if the decisional Diffie–Hellman problem is hard relative to $\mathcal{G}$.

[10%] 11.7 Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let $\mathbb{G}$ be the group of squares modulo p (so $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$ of order q), and let g be a generator of $\mathbb{G}$. The private key is $(\mathbb{G}, g, q, x)$ and the public key is $(\mathbb{G}, g, q, h)$, where $h = g^x$ and $x \in \mathbb{Z}_q$ is chosen uniformly. To encrypt a message $m \in \mathbb{Z}_q$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 := g^r \bmod p$ and $c_2 := h^r + m \bmod p$, and let the ciphertext be $\langle c_1, c_2 \rangle$. Is this scheme CPA-secure? Prove your answer.

Hint for 11.6 : Prove that if "not CPA-secure" then "DDH problem is efficiently solved ».

[10%] 11.13 One of the attacks on plain RSA discussed in Section 11.5.1 involves a sender who encrypts the same message to three different receivers. Formulate an appropriate definition of security ruling out such attacks, and show that any CPA-secure public-key encryption scheme satisfies your definition.

More on back…

[10%]

12.1 Show that Construction 4.7 for constructing a variable-length MAC from any fixed-length MAC can also be used (with appropriate modifications) to construct a signature scheme for arbitrary-length messages from any signature scheme for messages of fixed length $\ell(n) \geq n$.

12.5 Another approach (besides hashing) that has been tried to construct secure RSA-based signatures is to *encode* the message before applying the RSA permutation. Here the signer fixes a public encoding function $\mathsf{enc} : \{0,1\}^\ell \to \mathbb{Z}_N^*$ as part of its public key, and the signature on a message m is $\sigma := [\mathsf{enc}(m)^d \bmod N]$.

[5%] (a) How is verification performed in encoded RSA?

[5%] (b) Discuss why appropriate choice of encoding function for $\ell \ll \|N\|$ prevents the "no-message attack" described in Section 12.4.1.

[5%] (c) Show that encoded RSA is insecure if $\mathsf{enc}(m) = \mathtt{0x00}\|m\|0^{\kappa/10}$ (where $\kappa \stackrel{\text{def}}{=} \|N\|$, $\ell = |m| \stackrel{\text{def}}{=} 4\kappa/5$, and m is not the all-0 message). Assume $e = 3$.

[5%] (d) Show that encoded RSA is insecure for $\mathsf{enc}(m) = 0\|m\|0\|m$ (where $\ell = |m| \stackrel{\text{def}}{=} (\|N\| - 1)/2$ and m is not the all-0 message). Assume $e = 3$.

[5%] (e) Solve parts (c) and (d) for arbitrary e.

[10%]

12.11 The Lamport scheme uses 2ℓ values in the public key to sign messages of length ℓ. Consider the variant in which the private key contains 2ℓ values $x_1, \ldots, x_{2\ell}$ and the public key contains the values $y_1, \ldots, y_{2\ell}$ with $y_i := f(x_i)$. A message $m \in \{0,1\}^{\ell'}$ is mapped in a one-to-one fashion to a subset $S_m \subset \{1, \ldots, 2\ell\}$ of size ℓ. To sign m, the signer reveals $\{x_i\}_{i \in S_m}$. Prove that this gives a one-time-secure signature scheme. What is the maximum message length ℓ' that this scheme supports?

More on back…

M A T H E M A T I C A QUESTIONS

Let ***N***≔**1280188921986598694387442678917283771992957539817913990334601022593224943887566067283731210431548097902496634726772066225492472049090344014040948783013844255405121563940725271958261549105689512737212340197034018465582141671438383356743859483782939343644570817584684039164728765221998383240136062872083695440820**8209

be an RSA public modulus (***e*=*N*** as in Cocks‘ variation).

[10%] **1)** Without factoring ***N***, provide a message ***m*** that ends with “2018” in base 10 together with its **RSA** signature **σ**. Show that **σ** is a valid signature.

[10%] **2)** Without factoring ***N***, check that the exponent ***e′***≔**99985828020191359900880286869683035709839584003728838462445577041064925905995005216889007572898641811594513334409291762876864911044894074623553711135146 48093** is also valid to verify signed messages. Show at least **5** examples.

[10%] **3)** Given ***e*** and ***e′***, factor ***N***. What is special about the factors of ***N*** ?

More on back…