Exercise Sheet #7

Advanced Cryptography 2022

Exercise 1 DSS Security Hypothesis

We briefly recall the DSS signature algorithm:

Public parameters: pick a 160-bit prime number q, a large prime number $p = aq + 1$, a generator h of $\mathbb{Z}_p^*$ raised to the power a, $g = h^a \bmod p$ (an element of order q).

Set up: pick $x \in \mathbb{Z}_q$ and compute $y = g^x \bmod p$.

Secret key: $K_s = x$.

Public key: $K_p = y$.

Signature generation: pick a random $k \in \mathbb{Z}_q^*$, compute $r = (g^k \bmod p) \bmod q$, and $s = \frac{H(M)+xr}{k} \bmod q$. The signature is $\sigma = (r, s)$.

Verification: check that

$$r = \left(g^{\frac{H(M)}{s} \bmod q} y^{\frac{r}{s} \bmod q} \bmod p\right) \bmod q\ .$$

We consider the DSS signature algorithm with parameters p, q, g, a hash function H, and a public key y.

1. If the discrete logarithm problem is easy in the subgroup of $\mathbb{Z}_p^*$ spanned by g, show that anyone can forge signatures.

2. If H is not one-way, show that we can forge a (m, r, s) triplet so that (r, s) is a valid signature for the message m with the public key y.

3. If H is not collision resistant, show that we can forge a given signature with a chosen-message attack.

4. If the parameter k of DSS is predictable, show that we can deduce the secret key from a valid signature. What is the complexity of this attack when using brute force?

Exercise 2 Instances of the ElGamal (Final 2010)

Let p be a large prime number and g be an element of $\mathbf{Z}_p^*$. We denote by q the order of g. We let $\mathcal{G}$ be a subgroup of $\mathbf{Z}_p^*$ which includes g. We let $\mathcal{M} = \{0,1\}^\ell$ be the message space. We assume an injective function $e : \mathcal{M} \to \mathcal{G}$ which is called an *embedding function*. We further assume that given a random $m \in \mathcal{M}$, $e(m)$ "looks like" uniformly distributed in $\mathcal{G}$. In this exercise, we consider the ElGamal cryptosystem using domain parameters (p, g, q, e) with different choices on how to select them. Namely, a secret key is a value $x \in \mathbf{Z}_q$, its public key is $y = g^x \bmod p$. For any message $m \in \mathcal{M}$, the encryption of m with public key y is a pair (u, v) such that $u = g^r$ with $r \in \mathbf{Z}_q$ random and $v = e(m)y^r$. The decryption of (u, v) with secret key x is $m = e^{-1}(vu^{-x})$.

1. We assume here that g is a generator of $\mathbf{Z}_p^*$. What is the value of q?

   Is the cryptosystem IND-CPA secure? Why?

2. We assume here that q is a large prime but much smaller than p, and that $\mathcal{G}$ is generated by g.

   Is the cryptosystem IND-CPA secure? Why?

   In practice, is it easy to propose an efficient embedding function e?

3. We assume here that $p = 1 + 2q$ with q prime and that $\mathcal{G}$ is generated by g.

   Is the cryptosystem IND-CPA secure? Why?

   Show that $\mathcal{G}$ is the subgroup of all quadratic residues in $\mathbf{Z}_p^*$.

   Compute $\left(\frac{-1}{p}\right)$.

   Deduce that for any $x \in \mathbf{Z}_p^*$ then either x or $-x$ is in $\mathcal{G}$.

   Finally, if $\ell = \lfloor \log_2 q \rfloor$, propose a practical embedding function e.

Exercise 3 PIF Implies PAF (Final 2011)

We consider a function family F_k taking inputs of length λ, making outputs of length λ, and where the key k is also of length λ. We consider the two following games:

Game $\mathsf{PIF}(\mathcal{A}, 1^\lambda)$:

pick some random coins k of length λ
pick ρ
run $\mathcal{A}(\rho) \to x$
if $|x| \neq \lambda$, output 0 and stop
pick a random bit b
if $b = 0$ **then**
  compute $y = F_k(x)$
else
  pick a random y of λ bits
end if
run $\mathcal{A}(y; \rho) \to b'$
output $b \oplus b' \oplus 1$

Game $\mathsf{PAF}(\mathcal{A}, 1^\lambda)$:

pick some random coins k of length λ
pick ρ
pick a random x of length λ
compute $y = F_k(x)$
run $\mathcal{A}(y; \rho) \to x'$
output $1_{x=x'}$

We say that F_k is PIF-secure (resp. PAF-secure) if for all polynomially bounded $\mathcal{A}$, we have that $\Pr[\mathsf{PIF}(\mathcal{A}, 1^\lambda) = 1] - \frac{1}{2}$ (resp. $\Pr[\mathsf{PAF}(\mathcal{A}, 1^\lambda) = 1]$) is a negligible function in terms of λ.

Q.1 Show that if F_k is PIF-secure, then it is PAF-secure.

Hint: based on a PAF-adversary $\mathcal{A}$ and some coins $\rho' = r' \| \rho \| b''$, define $\mathcal{A}'(\rho') = x$ picked at random from r' then $\mathcal{A}'(y, \rho') = 1$ if $\mathcal{A}(y; \rho) = x$ and $\mathcal{A}'(y, \rho') = b''$ otherwise. By considering $\mathcal{A}'$ as a PIF-adversary, look at the link between $\Pr[\mathsf{PIF}(\mathcal{A}', 1^\lambda) = 1] - \frac{1}{2}$ and $\Pr[\mathsf{PAF}(\mathcal{A}, 1^\lambda) = 1]$.