The art of cryptography: security, reductions, and group cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

7. Assignment

(Due: Thursday, 24 May 2012, 13^{00})

Exercise 7.1 (notions of indistinguishability)**.** Let $\Pi = (\text{setup}, \text{enc}, \text{dec})$ be an asymmetric encryption scheme. In the lecture, we considered the following *distinguishing experiment* $\mathsf{Dist}_{\mathcal{A},\Pi}(n)$ for an attacker $\mathcal{A}$.

Experiment 1: the distinguishing experiment $\mathsf{Dist}_{\mathcal{A},\Pi}(n)$

Input: adversary $\mathcal{A}$, encryption scheme $\Pi = (\text{setup}, \text{enc}, \text{dec})$, security parameter n in unary
Output: bit b^*

1 Run setup(1^n) to obtain keys $(\mathsf{pk}, \mathsf{sk})$.
2 Adversary $\mathcal{A}$ is given pk and outputs a message x_0.
3 A message x_1 of the same length as x_0 is chosen uniformly at random.
4 A bit $b \xleftarrow{R} \{0,1\}$ is chosen uniformly at random.
5 The *challenge ciphertext* $c \leftarrow \text{enc}_{\mathsf{pk}}(m_b)$ is computed and given to $\mathcal{A}$.
6 $\mathcal{A}$ outputs a bit b^*.
7 Return b^*.

The success probability of an attacker $\mathcal{A}$ in the distinguishing game is

$$|\text{prob}\{\mathsf{Dist}_{\mathcal{A},\Pi}(n) = b\} - \frac{1}{2}|.$$

We say that Π has *indistinguishable encryptions* if for all probabilistic polynomial-time (ppt) adversaries $\mathcal{A}$ the success probability in the distinguishing game is negligible.

(i) (6 points) Let us give more power to the attacker. The *extended distinguishing experiment* $\mathsf{Dist}^*_{\mathcal{A},\Pi}(n)$ runs like $\mathsf{Dist}_{\mathcal{A},\Pi}(n)$ except that the message $x_1 \neq x_0$ in step 3 is also chosen by the attacker. The success probability in this experiment is analogously defined as $|\text{prob}\{\mathsf{Dist}^*_{\mathcal{A},\Pi}(n) = b\} - \frac{1}{2}|$.

Prove that Π has indistinguishable encryptions if and only if for all ppt adversaries $\mathcal{A}$ the success probability in the extended distinguishing experiment is negligible.

(ii) (6 points) An equivalent way of formalizing indistinguishility is to state that every adversary behaves the same way whether it sees an encryption of x_0 or x_1. Let $\mathsf{Dist}^*_{\mathcal{A},\Pi}(n,b)$ be the extended distinguishing experiment as in (i) except that the fixed bit b is used in step 4.

Prove that Π has indistinguishable encryptions if and only if for all ppt adversaries $\mathcal{A}$ the prob$\{\mathsf{Dist}^*_{\mathcal{A},\Pi}(n,1)) \neq \mathsf{Dist}^*_{\mathcal{A},\Pi}(n,0))\}$ is negligible.

Exercise 7.2 (ElGamal in action)**.** We use the ElGamal encryption system in the group $G = \mathbb{Z}_p^\times$ with prime $p = 20443$.

`A` is mapped to 0, `B` to 1 and so forth. We combine groups of three letters (a_0, a_1, a_2) to $a_0 + 26a_1 + 26^2 a_2$. Thus `ABC` corresponds to $0 + 26 \cdot 1 + 2 \cdot 26^2 = 1378$.

(i) (2 points) Show that $g = 2$ is a generator of G.

[Hint: An element $a \in \mathbb{Z}_p^\times$ is a generator if and only if $a^{(p-1)/t} \neq 1$ for all prime divisors t of $p-1$.]

(ii) (3 points) Alice has published the public key $g^{s_A} = 8224$. Your secret key is $s_B = 321$. Send her an encryption of the message `SYSTEM`.

(iii) (5 points) The following transcript of a conversation was intercepted, which contains a 3-part message encrypted with the ElGamal encryption system in $G = \mathbb{Z}_{20443}^\times$ with $g = 2$ (using the mapping from letters to numbers described above).

Alice	has the public key 7189.
Bob to Alice:	message (part 1) $(16278, 4151)$.
Bob to Alice:	message (part 2) $(12430, 4151)$.
Bob to Alice:	message (part 3) $(2689, 4151)$.

Obviously, the lazy cryptographer has made the mistake of choosing the same session key for all three messages. Furthermore, an indiscretion revealed that one part of the message corresponds to the clear text 8324. Compute the (alphabetic) clear text of the entire message.

Can you find the secret key?