Faculty of Science
Final Examination

Computer Science COMP-547A
Cryptography and Data Security

Examiner: Prof. Claude Crépeau
Associate Examiner: Prof. David Avis

Date: Dec 7th, 2005
Time: 14:00 – 17:00
Room: PetH 206

INSTRUCTION:
- This examination is worth 50% of your final grade.
- The total of all questions is 109 points.
- Each question is assigned a value found in parenthesis next to it.
- This is an open book examination. All documentation is permitted.
- Faculty standard calculator permitted only.
- This examination consists of 6 questions on 4 pages, including title page.

Suggestion: read all the questions and their values before you start.

Question 1. Easy bits (12 points)

Let **p** be an odd prime and **g** be a primitive element **mod p**.

- Show that given **p, g, g^x mod p**, the predicate **$lsb_p(x)$** is easy to compute.
- Show that given **p, g, g^a mod p, g^b mod p** there is a predicate of **g^{ab} mod p** that is easy to compute.

Question 2. Second Preimage (12 points)

4.6 Suppose that $f : \{0,1\}^m \rightarrow \{0,1\}^m$ is a preimage resistant bijection. Define $h : \{0,1\}^{2m} \rightarrow \{0,1\}^m$ as follows. Given $x \in \{0,1\}^{2m}$, write

$$x = x' \parallel x''$$

where $x', x'' \in \{0,1\}^m$. Then define

$$h(x) = f(x' \oplus x'').$$

Prove that h is not second preimage resistant.

Question 3. Blum-Goldwasser à la RSA (25 points)

Let **n=pq** be the product of two large primes such that **p ≡ q ≡ 2 (mod 3)**.

- Provide all the details of a variant of the Blum-Goldwasser cryptosystem where we use RSA with public exponent **3** (**z_i=lsb($s_0^{3^i}$ mod n)**) instead of BBS (**z_i=lsb($s_0^{2^i}$ mod n)**) as in the original system. Rewrite the entire description of the Blum-Goldwasser cryptosystem as given in cryptosystem 8.2 (see next page).
- Explain why choosing exponent 3 is a better choice than an arbitrary RSA exponent.
- Explain why we requested **p ≡ q ≡ 2 (mod 3)**.
- Compare the security of the resulting system to the security of the original system.

Cryptosystem 8.2: *Blum-Goldwasser Public-key Cryptosystem*

Let $n = pq$, where p and q are primes, $p \equiv q \equiv 3 \pmod 4$. The integer n is public; the factorization $n = pq$ is secret. Let $\mathcal{P} = (\mathbb{Z}_2)^\ell$, $\mathcal{C} = (\mathbb{Z}_2)^\ell \times {\mathbb{Z}_n}^*$ and $\mathcal{R} = {\mathbb{Z}_n}^*$. Define $\mathcal{K} = \{(n, p, q)\}$, where n, p and q are as defined above. For $K = (n, p, q)$, $x \in (\mathbb{Z}_2)^\ell$ and $r \in {\mathbb{Z}_n}^*$, encrypt x as follows:

1. Compute $z_1, \ldots, z_\ell$ from seed $s_0 = r$ using the *BBS Generator*.
2. Compute $s_{\ell+1} = {s_0}^{2^{\ell+1}} \bmod n$.
3. Compute $y_i = (x_i + z_i) \bmod 2$ for $1 \leq i \leq \ell$.
4. Define $e_K(x, r) = (y_1, \ldots, y_\ell, s_{\ell+1})$.

To decrypt y, Bob performs the following steps:

1. Compute $a_1 = ((p + 1)/4)^{\ell+1} \bmod (p - 1)$.
2. Compute $a_2 = ((q + 1)/4)^{\ell+1} \bmod (q - 1)$.
3. Compute $b_1 = {s_{\ell+1}}^{a_1} \bmod p$.
4. Compute $b_2 = {s_{\ell+1}}^{a_2} \bmod q$.
5. Use the Chinese remainder theorem to find r such that

$$r \equiv b_1 \pmod p$$

and

$$r \equiv b_2 \pmod q.$$

6. Compute $z_1, \ldots, z_\ell$ from seed $s_0 = r$ using the *BBS Generator*.
7. Compute $x_i = (y_i + z_i) \bmod 2$ for $1 \leq i \leq \ell$.
8. The plaintext is $x = (x_1, \ldots, x_\ell)$.

Question 4. One-time padding (20 points)

Consider the following cryptosystem $\mathbf{P=K=C=\{1,2,\ldots,p-1\}}$ for a prime $\mathbf{p}$:

$$E_k(x) = kx \bmod p \text{ and } D_k(y) = k^{-1}y \bmod p$$

- Show that this cryptosystem is a perfect cipher.

- Show that for $\mathbf{p=3}$ this cryptosystem is such that $\mathbf{E_k(x) = D_k(x)}$.

- Show also that essentially for $\mathbf{p=3}$ this cryptosystem is the same as the binary one-time pad where $\mathbf{y=x\oplus k}$.

Question 5. Short and *Sweet* (25 points)

(a) (5 points)
Explain why the RSA signature scheme is not resistant to existential forgeries?

(b) (5 points)
What is the unicity distance of a **1024** modulus RSA crypto-system?

(c) (5 points)
Explain how we could break RSA if we could extract discrete logs modulo $\mathbf{n=p*q}$.

(d) (10 points)
In Rabin's cryptosystem, the encryption function is $\mathbf{Rabi_n(x)=x^2 \bmod n}$, with $\mathbf{n=p*q}$. The decryption function consists of extracting the square root of $\mathbf{Rabi_n(x)}$, which we can do efficiently given **p** and **q**. Consider the following extension of Rabin's crypto-system, named RRSA (Rabin-RSA): let **e** be a public exponent and **d** a private exponent such that $\mathbf{e*d \bmod \phi(n) = 2}$ for $\mathbf{n=p*q}$, the product of two large primes.

- Show that $\mathbf{(x^e)^d \bmod n = Rabi_n(x)}$ for any **x**, $\mathbf{0<x<n}$.
- Compare the security of RRSA to RSA and Rabin cryptosystems.

Question 6. Information Theory (15 points)

Let **P** be the random variable for the plaintext messages, **C** be the random variable for the ciphertext messages, and **K** be the random variable for the keys of a cryptosystem.

- Prove the following statement $\mathbf{H(C|K,P)=H(P|K,C)}$.

- Why is the assumption $\mathbf{I(P;K)=0}$, usually made about cryptosystems?

- If we have a public-key cryptosystem, let $\mathbf{K_e}$ and $\mathbf{K_d}$ be the random variables for the public (encryption) key and private (decryption) key.
What are the values of $\mathbf{H(K_d|K_e)}$ and $\mathbf{I(K_e;K_d)}$??