Advanced Cryptography — Midterm Exam

Serge Vaudenay

17.4.2012

- duration: 3h00
- any document is allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will not answer any technical question during the exam
- the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

1 Circular RSA Encryption

Let $n = pq$ and $d = e^{-1} \bmod \varphi(n)$ define an RSA key pair. For some reason, we need to encrypt p with the plain RSA cryptosystem.

Q.1 If y decrypts to p, show that an adversary who has only the public key at disposal can decrypt y.
Hint: think modulo p.

2 The Goldwasser-Micali Cryptosystem

Consider the group $\mathbf{Z}_n^*$. We recall that if m is an odd factor of n, then the Jacobi symbol $x \mapsto \left(\frac{x}{m}\right)$ is a group homomorphism from $\mathbf{Z}_n^*$ to $\{-1,+1\}$. I.e., $\left(\frac{xy \bmod n}{m}\right) = \left(\frac{x}{m}\right)\left(\frac{y}{m}\right)$. It further has the property that $\left(\frac{x}{mm'}\right) = \left(\frac{x}{m}\right)\left(\frac{x}{m'}\right)$. We consider that multiplication in $\mathbf{Z}_n$ and the computation of the above Jacobi symbol can each be done in $O((\log n)^2)$.

Let s be a security parameter. We consider the following public-key cryptosystem.

Key Generation. Generate two different odd prime numbers p and q of bit size s, compute $n = pq$, and find some $z \in \mathbf{Z}_n^*$ such that $\left(\frac{z}{p}\right) = \left(\frac{z}{q}\right) = -1$. The public key is (n,z) and the secret key is p.

Encryption. To encrypt a bit $b \in \{0,1\}$, pick $r \in_U \mathbf{Z}_n^*$ and compute $c = r^2 z^b \bmod n$. The ciphertext is c.

Decryption. To decrypt c, compute $\left(\frac{c}{p}\right)$ and find b such that it equals $(-1)^b$. The plaintext is b.

This cryptosystem is known as the Goldwasser-Micali cryptosystem.

Q.1 Show that the cryptosystem is correct. I.e., if the key generation gives (n,z) and p, if b is any bit, if the encryption of b with the key (n,z) produces c, then the decryption of c with the key p produces b.

Q.2 Analyze the complexity of the three algorithms in terms of s.

Q.3 Let $\mathcal{N}$ be the set of all n's which could be generated by the key generation algorithm. Let Fact be the problem in which an instance is specified by $n \in \mathcal{N}$ and the solution is the factoring of n.

Q.3a Define the key recovery problem KR related to the cryptosystem. For this, specify clearly what is its set of instances and what is the solution of a given instance.

Q.3b Show that the KR problem is equivalent to the Fact problem. Give the actual Turing reduction in both directions.

Q.4 Let QR be the problem in which an instance is specified by a pair (n,c) in which $n \in \mathcal{N}$ and $\left(\frac{c}{n}\right) = 1$. The problem is to decide whether or not c is a quadratic residue in $\mathbf{Z}_n^*$.

Q.4a Define the decryption problem DP related to the cryptosystem. For this, specify clearly what is its set of instances and what is the solution of a given instance.

Q.4b Show that the DP problem is equivalent to the QR problem. Give the actual Turing reduction in both directions.

3 Faulty Multiplier

Let B be a basis. Given some integers $x_0,\ldots,x_{n-1}$, we say that the sequence $[x_{n-1},\ldots,x_0]$ represents x if

$$x = \sum_{i=0}^{n-1} x_i B^i$$

We say that $[x_{n-1},\ldots,x_0]$ is a reduced sequence if $0 \le x_i \le B-1$ for all $i = 0,\ldots,n-1$. We say that a number x contains a block a if there exists n and a reduced sequence $[x_{n-1},\ldots,x_0]$ representing x, and some i such that $a = x_i$. We consider the schoolbook algorithms for addition and multiplication. These are the methods that children learn at school for $B = 10$ and reduced sequences. We extend them to any B value.

We work with a microprocessor using a built-in 32×32-bit to 64-bit hardware multiplication. Each 32×32-bit to 64-bit multiplication is called an elementary multiplication. So, in the next we let $B = 2^{32}$. We assume that there is a bug such that the result is always correct except when the first operand is a special a_0 value and the second one is a special b_0 value in which case the result is a constant c_0 which is not equal to $a_0 b_0$.

Q.1 Let a,b,c,u,v be five 32-bit blocks. Let x be represented by $[a,b,c]$ and y be represented by $[u,v]$. Using the schoolbook multiplication algorithm in basis B to multiply x by y, give the list of elementary multiplications which are required to compute xy.

Q.2 Let $w = \left\lceil \frac{\sqrt{b_0 B^3} - a_0}{B} \right\rceil$ and y be represented by $[w, a_0]$. Assume that $b_0 \le \frac{B}{4} - 1$. Deduce that y contains the block a_0 and that y^2 contains the block b_0.
Hint: first show that

$$\sqrt{(b_0+1)B} - \sqrt{b_0 B} \ge 1$$

then show that

$$\frac{\sqrt{(b_0+1)B^3} - a_0}{B} > w \ge \frac{\sqrt{b_0 B^3} - a_0}{B}$$

and deduce that $\sqrt{(b_0+1)B^3} > y \ge \sqrt{b_0 B^3}$.
In what follows, we assume that y does not contain the block b_0 and that y^2 does not contain the block a_0.

Q.3 Assume we want to raise y to some power k modulo n using the square-and-multiply with scanning of the bits of the exponent from left to right. The leading bit of the exponent k being 1, let b denote the second leading bit of k.

Q.3a Give the list of all multiplications this algorithm does when scanning these two bits in the two cases: i.e., for $b = 0$ and $b = 1$.

Q.3b Show that for the y from Q.2, this algorithm is likely to compute $y^k \bmod n$ correctly when $b = 0$ whereas it does a computation error when $b = 1$.

Q.4 We assume a tamper-proof device implementing the RSA decryption with CRT acceleration, square-and-multiply with scanning of the bits of the exponent from left to right, and the schoolbook multiplication algorithm.

Q.4a Assuming that the second leading bits of $d \bmod (p-1)$ and $d \bmod (q-1)$ are different, using the y of Q.2, give an algorithm producing x such that $x^e \bmod n$ is equal to y modulo either p or q but not modulo both.

Q.4b Deduce a factoring attack on RSA using this device.

4 Trapdoor Sbox

Let n be an integer. We consider the set $\mathbf{Z}_2^n$ as a vector space. Given a vector x, x_k denotes its k-th component (which is a bit). Additions are implicitly takes modulo 2. Product of bits are also implicitly taken modulo 2. The dot product $\alpha \cdot x$ between two vectors means $\sum_{k=1}^n \alpha_k x_k$. We also multiply a bit by a vector by multiplying the bit to each component.

Let $\alpha, \beta, \gamma \in \mathbf{Z}_2^n$. Let i and j be two fixed indices such that $\alpha_i = \beta_j = 1$ and $\gamma_j = 0$. Let w be the total number of bits set to 1 in γ. Let A be the subset of $\mathbf{Z}_2^n$ of all tuples in which the i-th component is zero. Let B be the subset of $\mathbf{Z}_2^n$ of all tuples in which the j-th component is zero. Let φ be a bijection from A to B.

Let p be a function from $\mathbf{Z}_2^n$ to A defined by $p(x)_k = x_k$ for all $k \neq i$ and $p(x)_i = 0$.

Let $v = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbf{Z}_2^n$ be a constant vector, where $v_j = 1$.

We construct a function S on $\mathbf{Z}_2^n$ as follows.

$$S(x) = \varphi(p(x)) + \left((\alpha \cdot x) + (\beta \cdot \varphi(p(x))) + \prod_{k:\gamma_k=1} \varphi(p(x))_k \right) v$$

Q.1 Show that S is a permutation.
Hint: show that $S(x) = S(x')$ implies $p(x) = p(x')$ for any x and x' and show that $S(x+u) = S(x) + v$ for a constant vector u and any x.

Q.2 Compute $\mathsf{LP}_S(\alpha, \beta)$.
Hint: first give a simple expression of $(\alpha \cdot x) + (\beta \cdot S(x))$.

Q.3 Deduce a way to construct an Sbox with a given high $\mathsf{LP}_S(\alpha, \beta)$.