System and Network Security (CS 5470)

Quiz - 1 (Spring 2025)

International Institute of Information Technology, Hyderabad

Time: 1 Hour and 10 Minutes Total Marks: 20

Instructions: Answer *ALL* questions.

This is a closed books and notes examination.

Write your answers sequentially as given in the question paper and also all the parts of a question at the same place.

No query is allowed in the examination hall.

NO mobile phone/device is permitted.

Use of Regular Calculator is allowed.

4 Feb 2025

1. Suppose you being Alice and Bob agree on secure communication using the RSA public key cryptosystem. You wish to send a plaintext M to Bob using the RSA algorithm. Let the public key for Bob be the pair $(n, e) = (187, 7)$. Note that $187 = 17 \times 11$ and $7 \times 23 \equiv 1 \pmod{160}$. The following standard encoding procedure is used:

   A = 01, B = 02, . . ., Z = 26,

   , = 27, . = 28, ? = 29,

   0 = 30, 1 = 31, . . ., 9 = 39, ! = 40,

   with 00 indicating a space between words.

   Assume that you want to transmit the message (last four digits of your roll number) in blocks.

   (a) What will be the ciphertext to be produced with your roll number as the encoded plaintext message?

   (b) Show that Bob will recover the original plaintext using the RSA decryption.

   [(4+4) = 8]

   Solution: Here, $e = 7$, $d = 23$ and $n = 187$. Public key $(n, e) = (187, 7)$ and private key $(n, d) = (187, 23)$.

   (a) Suppose a student's roll number is 2024202012 and the last four digits of the roll number as plaintext is $P = 2012$. Since $n = 187$, we have the blocks of optimal size in this case is 2 and hence, the plaintext blocks are $P_1 = 20$ and $P_2 = 12$.

   The ciphertext blocks are then $C_1 = P_1^e \pmod{n} = 20^7 \pmod{187} = 147$, and $C_2 = P_2^e \pmod{n} = 12^7 \pmod{187} = 177$, using the repeated square-and-multiply algorithm. Thus, the ciphetext is $C_1C_2 = 147177$.

(b) The recovered plaintext blocks are $P_1 = C_1^d \pmod n = 147^{23} \pmod{187} = 20$, and $P_2 = C_2^d \pmod n = 177^{23} \pmod{187} = 12$, using the repeated square-and-multiply algorithm. The original plaintext would be $P = P_1P_2 = 2012$.

2. The fundamental theorem of arithmetic states that any positive interger $n > 1$ can be UNIQUELY expressed in the form:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

where $p_1 < p_2 < \cdots < p_r$ are prime numbers and where each a_i is a positive integer.

Using this, compute $\phi(11011)$.

[4]

Solution: We have: $11011 = 7 * 11^2 * 13$. If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$,

$$\begin{aligned} \phi(n) &= p_1^{a_1}(1 - \frac{1}{p_1}) * p_2^{a_2}(1 - \frac{1}{p_2}) * \cdots * p_r^{a_r}(1 - \frac{1}{p_r}) \\ &= n * (1 - \frac{1}{p_1}) * (1 - \frac{1}{p_2}) * \cdots * (1 - \frac{1}{p_r}). \end{aligned}$$

Hence, $\phi(11011) = 11011 * (1 - 1/7) * (1 - 1/11) * (1 - 1/13) = 7920$.

A user A selects two large primes p and q of almost equal length such that the factorization of $n = pq$ is infeasible. He selects a basis $g_p, g_q \in \{1, \ldots, n-1\}$ of $\mathbb{Z}_n^*$ with $\text{ord}_n(g_p) = p - 1$, $\text{ord}_n(g_q) = q - 1$ and two distinct primes π_p, π_q dividing $p - 1$ and $q - 1$, respectively. He computes $\gamma_p = g_p^{(p-1)/\pi_p} \bmod n$ and $\gamma_q = g_q^{(q-1)/\pi_q} \bmod n$. Next, he selects arbitrary numbers $b_p \in \{0, \ldots, \pi_p - 1\}$, $b_q \in \{0, \ldots, \pi_q - 1\}$ and computes $y_p = \gamma_p^{b_p} \bmod n$, $y_q = \gamma_q^{b_q} \bmod n$. Finally, he consider a publicly known hash function $h : \{0,1\}^* \to \{1, \ldots, m\}$, where m is an integer with $m < \pi_p\pi_q$. The public key of A is $(m, n, \gamma_p, \gamma_q, y_p, y_q)$ and its private key $(p, q, \pi_p, \pi_q, b_p, b_q)$.

Figure 1: Public and private key generation phase

Suppose A wants to sign a message $x \in M$ using his private key. First, he selects (secret) random integers $z_p \in \{0, \ldots, \pi_p - 1\}$, $z_q \in \{0, \ldots, \pi_q - 1\}$ and computes

$$R = \gamma_p^{z_p} \gamma_q^{z_q} \bmod n.$$

Next, he computes

$$S_p = z_p^{-1}(h(x) + Rb_p) \bmod \pi_p, \quad S_q = z_q^{-1}(h(x) + Rb_q) \bmod \pi_q.$$

The signature of x is (R, S_p, S_q). A sends the message x with its signature (R, S_p, S_q) to B.

Figure 2: Signature generation phase

3. Assume that two participants, say A and B agree on the following variant of Digital Signature Algorithm (DSA) based on the group $Z_n^* = \{1, 2, \cdots, n-1\}$, where n is the product of two primes such that its factorization is infeasible. Figure 1 shows the "public and private key generation" phase by the user A, whereas Figure 2 represents the "signature generation" phase by the user A.

   Design a verification algorithm for the verifier B. Also, provide the correctness proof of the verification algorithm.

   [(6 + 2) = 8]

   Solution: See Section 3.3 of the attached research paper: "A variant of Digital Signature Algorithm".

********** **End of Question Paper** **********

Des. Codes Cryptogr. (2009) 51:99–104
DOI 10.1007/s10623-008-9246-y

A variant of Digital Signature Algorithm

Dimitrios Poulakis

Received: 5 September 2008 / Revised: 5 September 2008 / Accepted: 7 October 2008 /
Published online: 19 November 2008

Abstract In this paper we present a variant of the Digital Signature Algorithm based on a factorization problem and two discrete logarithm problems. We prove that our signature scheme is at least as secure as the original Digital Signature Algorithm and withstands all known attacks.

Keywords Public key cryptography · ElGamal signature · Digital Signature Algorithm · Discrete logarithm · Factorization

Mathematics Subject Classification (2000) 94A60

1 Introduction

In 1985, ElGamal proposed a public key cryptosystem and a digital signature scheme based on the difficulty of solving the Discrete Logarithm Problem in the multiplicative group of an appropriate finite field $\mathbb{Z}_p$ [3]. The National Institute of Standards and Technology of USA proposed the Digital Signature Algorithm (DSA) which is an efficient variant of the ElGamal digital signature scheme [8,9].

Let us recall the outlines of DSA. The signer chooses a prime p of size between 512 and 1024 bits with increments of 64, q is a prime of size 160 with $q|p-1$ and g is a generator of the unique order q subgroup G of $\mathbb{Z}_p^*$. Further, he chooses $a \in \{1,\ldots,q-1\}$ and computes $A = g^a \bmod p$. The public key of the signer is (p, q, g, A) and his private key a. Furthermore, the signer chooses a publicly known hash function h mapping messages to $\{0,\ldots,q-1\}$. To sign a message m, he chooses a random number $k \in \{1,\ldots,q-1\}$,

Communicated by P. Wild.

D. Poulakis (✉)
Department of Mathematics, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece
e-mail: poulakis@math.auth.gr

computes $r = (g^k \bmod p) \bmod q$ and sets $s = k^{-1}(h(m) + ar) \bmod q$. The signature of m is (r, s). The verification of the signature is performed by checking

$$r = ((g^{s^{-1}h(m) \bmod q} A^{s^{-1}r \bmod q}) \bmod p) \bmod q.$$

Notice that the secrecy of k is crucial. If k is revealed to the adversary, then the latter can recover the secret key a. Thus, the parameters of the system were chosen in such a way that the computation of discrete logarithms in $\mathbb{Z}_p^*$ and in G is computationally infeasible, and so a or k is well protected. However, serious precautions must be taken when using DSA in order to avoid the attacks given in [1,2,5,10]. A common feature of these attacks is that take advantage of the form of equality $s = k^{-1}(h(m) + ar) \bmod q$.

In this paper, we present a version of the DSA which combines the intractability of the integer factorization problem and discrete logarithm problem, and it is at least as secure as DSA. It uses computations in the group $\mathbb{Z}_n^*$, where n is the product of two large primes. For the verification of a signature in our signature scheme, the prime factorization of n is not required. Thus, we consider the prime factors of n as a part of the private key, and so we can hide the order of underlying group. An immediate consequence of this fact is that the above mentioned attacks do not longer work.

Note that modifications of ElGamal signature to work with composite module are given in [4], [7, Sect. 3], [11,12]. The construction of our variant of DSA does not follow the same approach. The main difference is that our scheme uses the full structure of $\mathbb{Z}_n^*$ as finitely generated abelian group and not only a cyclic subgroup of $\mathbb{Z}_n^*$, as the above schemes. Thus, an attacker has to solve except a factorization problem and two discrete logarithm problems instead of one as in the aforementioned schemes.

The paper is organized as follows. In Sect. 2 we recall the bases of $\mathbb{Z}_n^*$ which are necessary for our construction. In Sect. 3, we present our signature scheme. In Sect. 4 we deal with its security. Finally, in Sect. 5 we analyze its performance.

2 Bases of $\mathbb{Z}_n^*$

In this section we recall some facts from number theory. Let m be a positive integer. For every $x \in \mathbb{Z}$, we denote by $[x]_m$ the class of x in $\mathbb{Z}_m$ and by $\mathrm{ord}_m(x)$ the order of $x \pmod m$. For $w \in \mathbb{Z}_m^*$, we denote by $< w >$ the cyclic subgroup of $\mathbb{Z}_m^*$ generated by x. Finally, ϕ denotes the Euler's totient function.

Now, let n be an odd integer and $n = p_1^{a_1} \cdots p_k^{a_k}$ its prime factorization. By [6, Theorem 4.9], the map

$$f : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_{p_1^{a_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{a_k}}^*, \ [x]_n \longmapsto \left([x]_{p_1^{a_1}}, \ldots, [x]_{p_k^{a_k}}\right)$$

is a group isomorphism. Then there exist integers $g_1, \ldots, g_k$ with $\mathrm{ord}_n(g_i) = \phi(p_i^{a_i})$ $(i = 1, \ldots, k)$ such that for every $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$ there are uniquely determined integers $n_1, \ldots, n_k$ with $0 \le n_i < \phi(p_i^{a_i})$ satisfying

$$x \equiv g_1^{n_1} \cdots g_k^{n_k} \pmod n.$$

We call the set $\{g_1, \ldots, g_k\}$ basis of $\mathbb{Z}_n^*$. Thus, the group $\mathbb{Z}_n^*$ is the direct sum of cyclic groups $< [g_i]_n >$ $(i = 1, \ldots, k)$. So, if we have a congruence of the form

$$g_1^{l_1} \cdots g_k^{l_k} \equiv g_1^{n_1} \cdots g_k^{n_k} \pmod n,$$

then $l_i \equiv n_i \pmod{\phi(p_i^{a_i})} (i = 1, \ldots, k)$.

A basis of $\mathbb{Z}_n^*$ can be obtained as follows. If γ_i is a primitive root (mod $p_i^{a_i}$), then the integer g_i with $g_i \equiv \gamma_i \pmod{p_i^{a_i}}$ and $g_i \equiv 1 \pmod{p_j^{a_j}}$ for $j \in \{1, \ldots, i-1, i+1, \ldots, k\}$ has $\text{ord}_n(g_i) = \phi(p_i^{a_i})$ and so, $\{g_1, \ldots, g_k\}$ is a basis of $\mathbb{Z}_n^*$.

3 The proposed signature scheme

In this section we present a variant of Digital Signature Algorithm based on the group $\mathbb{Z}_n^*$, where n is the product of two primes such that its factorization is infeasible.

3.1 Public and private key generation

A user A selects two large primes p and q of almost equal length such that the factorization of $n = pq$ is infeasible. He selects a basis $g_p, g_q \in \{1, \ldots, n-1\}$ of $\mathbb{Z}_n^*$ with $\text{ord}_n(g_p) = p-1$, $\text{ord}_n(g_q) = q-1$ and two distinct primes π_p, π_q dividing $p-1$ and $q-1$, respectively. He computes $\gamma_p = g_p^{(p-1)/\pi_p} \bmod n$ and $\gamma_q = g_q^{(q-1)/\pi_q} \bmod n$. Next, he selects arbitrary numbers $b_p \in \{0, \ldots, \pi_p - 1\}$, $b_q \in \{0, \ldots, \pi_q - 1\}$ and computes $y_p = \gamma_p^{b_p} \bmod n$, $y_q = \gamma_q^{b_q} \bmod n$. Finally, he consider a publicly known hash function $h : \{0,1\}^* \to \{1, \ldots, m\}$, where m is an integer with $m < \pi_p \pi_q$. The public key of A is $(m, n, \gamma_p, \gamma_q, y_p, y_q)$ and its private key $(p, q, \pi_p, \pi_q, b_p, b_q)$.

3.2 Signature generation

Suppose A wants to sign a message $x \in M$ using his private key. First, he selects (secret) random integers $z_p \in \{0, \ldots, \pi_p - 1\}$, $z_q \in \{0, \ldots, \pi_q - 1\}$ and computes

$$R = \gamma_p^{z_p} \gamma_q^{z_q} \bmod n.$$

Next, he computes

$$S_p = z_p^{-1}(h(x) + Rb_p) \bmod \pi_p, \quad S_q = z_q^{-1}(h(x) + Rb_q) \bmod \pi_q.$$

The signature of x is (R, S_p, S_q). A sends the message x with its signature (R, S_p, S_q) to B.

3.3 Verification

B uses the public key of A verifies that

$$R = (\gamma_p^{h(x)} y_p^R)^{S_p^{-1}} (\gamma_q^{h(x)} y_q^R)^{S_q^{-1}} \bmod n.$$

If this equality is satisfied, then he accepts the signed message. Otherwise, he rejects it.

Proof of correctness of verification If R and S are computed as above we have

$$(\gamma_p^{h(x)} y_p^R)^{S_p^{-1}} (\gamma_q^{h(x)} y_q^R)^{S_q^{-1}} \equiv \gamma_p^{(h(x)+b_p R)s_p^{-1}} \gamma_q^{(h(x)+b_q R)s_q^{-1}} \equiv \gamma_p^{z_p} \gamma_q^{z_q} \pmod{n}$$

and hence

$$R = (\gamma_p^{h(x)} y_p^R)^{S_p^{-1}} (\gamma_q^{h(x)} y_q^R)^{S_q^{-1}} \bmod n.$$

Conversely, suppose the integers $R \in \{1, \ldots, n-1\}$, $S_p \in \{1, \ldots, \pi_p - 1\}$, $S_q \in \{1, \ldots, \pi_q - 1\}$ satisfy the previous equality. Then, there are $z_p \in \{0, \ldots, \pi_p - 1\}$, $z_q \in \{0, \ldots, \pi_q - 1\}$ such that

$$R = \gamma_p^{z_p}\gamma_q^{z_q} \bmod n.$$

On the other hand, there are $b_p \in \{0, \ldots, \pi_p - 1\}$, $b_q \in \{0, \ldots, \pi_q - 1\}$ with $y_p = \gamma_p^{b_p} \pmod n$ and $y_q = \gamma_q^{b_q} \pmod n$. Thus, we get

$$\gamma_p^{z_p}\gamma_q^{z_q} \equiv (\gamma_p^{h(x)}y_p^R)^{S_p^{-1}}(\gamma_q^{h(x)}y_q^R)^{S_q^{-1}} \equiv \gamma_p^{(h(x)+b_pR)S_p^{-1}}\gamma_q^{(h(x)+b_qR)S_q^{-1}} \pmod n,$$

whence we deduce

$$z_p \equiv (x + b_pR)S_p^{-1} \pmod{\pi_p}, \quad z_q \equiv (x + b_qR)S_q^{-1} \pmod{\pi_q}.$$

Therefore, (R, S_p, S_q) is the signature of the message x.

4 Security

An attacker, in order to recover the private key $(p, q, \pi_p, \pi_q, b_p, b_q)$ of A, has first to factorize n and find p and q. Next, he determines $\mathrm{ord_n}(\gamma_p) = \pi_p$ by computing the powers $\gamma_p^d \bmod n$, where d is a positive divisor of $p-1$. Similarly, he computes π_q. Finally, he has to compute the discrete logarithmes b_p and b_q of y_p and y_q to the bases γ_p and γ_q, respectively. Alternatively, if the attacker posses a signed message and knows z_p and z_q, then he easily obtains b_p and b_q. The quantities z_p and z_q can be computed from the equality

$$R = \gamma_p^{z_p}\gamma_q^{z_q} \bmod n.$$

Since p and q are known to the attacker, he gets

$$R^{p-1} \equiv (\gamma_q^{p-1})^{z_q} \pmod n, \quad R^{q-1} \equiv (\gamma_p^{q-1})^{z_p} \pmod n.$$

So, the attacker, in every case, has to solve two discrete logarithm problems.

Put $d = \gcd((p-1)/2, (q-1)/2)$. Suppose that $\{g_p, g_q\}$ is a basis of $\mathbb{Z}_n^*$ with $\mathrm{ord}_n(g_p) = p - 1$ and $\mathrm{ord}_n(g_q) = q - 1$. It is easily seen that we have either $\gcd(g_p^d - 1, n) = q$ or $\gcd(g_q^d - 1, n) = p$ and so, p, q and g_p, g_q must been choosen so that d is quite big and $\mathrm{ord}_q(g_p) = \mathrm{ord}_p(g_q) = d$.

Thus, the signer must take all necessary measures such that the factorization of n and the computation of discrete logarithm in the cyclic groups $< \gamma_p >$ and $< \gamma_q >$ to be infeasible. Since the primes π_p and π_q is a part of the private key, the attacks mentioned in the Introduction do not work in our scheme. The hash function protects our scheme from existential forgery in case where an attacker obtains the primes p, q, π_p, π_q. If π_p and π_q are known and the same couple (z_p, z_q) is used for two different messages, then b_p and b_q can easily be recovered, as in case of the original DSA. Thus, it is necessary to choose a new couple (z_p, z_q) for each new message.

Next, we shall show that our signature scheme is as secure as Digital Signature Algorithm. We say that an oracle O breaks a signature scheme, if given the public key of the scheme and a message x, it gives the corresponding signature for x.

Theorem 1 *If there is an oracle that can break our signature scheme, then it can also break DSA.*

Proof Let (p, q, g, A), a be a public key and a corresponding private key of DSA, respectively (as in the introduction), and $h(x) \in \{0, \ldots, q - 1\}$. We consider primes p', q' such that q' divides $p' - 1$ and g' is a generator of the unique subgroup of order q' of $\mathbb{Z}_{p'}^*$. Put

$n = pp'$. Let $\gamma_p, \gamma_{p'} \in \{1, \ldots, n-1\}$ such that $\gamma_p \equiv g \pmod{p}$, $\gamma_p \equiv 1 \pmod{p'}$, $\gamma_{p'} \equiv 1 \pmod{p}$, $\gamma_{p'} \equiv g' \pmod{p'}$. Let $y_p \in \{1, \ldots, n-1\}$ with $y_p \equiv A \pmod{p}$ and $y_p \equiv 1 \pmod{p'}$. Then $y_p = \gamma_p^a \bmod n$. Further, we choose $a' \in \{0, \ldots, q'-1\}$ and we put $y'_p = \gamma_{p'}^{a'} \bmod n$. Finally, take an integer m with $q < m < qq'$. Thus we have construct the public key $(m, n, \gamma_p, \gamma_{p'}, y_p, y'_p)$ for our signature scheme.

The oracle O gives a signature $(R, S_p, S_{p'})$ for the message x. Then we have

$$R = (\gamma_p^{S_p^{-1}h(x)} y_p^{S_p^{-1}R})(\gamma_{p'}^{S_{p'}^{-1}h(x)} y_{p'}^{S_{p'}^{-1}R}) \bmod n.$$

On the other hand, there are $z_p \in \{0, \ldots, q-1\}$, $z_{p'} \in \{0, \ldots, q'-1\}$ such that

$$R = \gamma_p^{z_p} \gamma_{p'}^{z_{p'}} \bmod n.$$

Thus,

$$\gamma_p^{z_p} \gamma_{p'}^{z'_p} \equiv \gamma_p^{S_p^{-1}(h(x)+aR)} \gamma_{p'}^{S_{p'}^{-1}(h(x)+a'R)} \pmod{n},$$

whence we get

$$z_p \equiv S_p^{-1}(h(x) + aR) \pmod{q},$$

and so we have

$$R \equiv \gamma_p^{z_p} \equiv \gamma_p^{S_p^{-1}h(x)} y_p^{S_p^{-1}R} \pmod{p}.$$

Put $r = (R \bmod p) \bmod q$ and $s = S_p \bmod q$. Hence, we deduce

$$r = (\gamma_p^{s^{-1}x} y_p^{s^{-1}r} \bmod p) \bmod q.$$

Therefore, the couple (r, s) is a valid DSA signature for x.

5 Performance analysis

The signature generation algorithm for our scheme is relatively fast. It requires two modular exponentiations $\gamma_p^{z_p} \bmod n$, $\gamma_q^{z_q} \bmod n$ and a modular multiplication for computing R. Further, it requires two applications of the extended Euclidean algorithm for computation of $z_p^{-1} \bmod \pi_p$, $z_q^{-1} \bmod \pi_q$, four modular multiplication and two modular additions for computing S_p and S_q. The computation of R, $z_p^{-1} \bmod \pi_p$, $z_q^{-1} \bmod \pi_q$, $Rb_p \bmod \pi_p$ and $Rb_q \bmod \pi_q$ can be done off-line. Thus, the signature generation requires only two modular multiplications and two modular additions. The signature verification needs six modular expontiations and three modular multiplications.

References

1. Bellare M., Goldwasser S., Micciancio D.: "Pseudo-random" number generation within cryptographic algorithms: the DSS case. In: Proceedings of Crypto '97, LNCS 1294. IACR, Palo Alto, CA. Springer-Verlag, Berlin (1997).
2. Blake I.F., Garefalakis T.: On the security of the digital signature algorithm. In honour of Ronald C. Mullin. Des. Codes Cryptogr. **26**(1–3), 87–96 (2002).
3. ElGamal T.: A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Trans. Inform. Theory **31**, 469–472 (1985).

4. Horster P., Michels M., Petersen H.: Meta-ElGamal signature schemes using a composite module. Technical Report TR-94-16-E, University of Technology Chemnitz-Zwickau. November 1994.
5. Howgrave-Graham N.A., Smart N.P.: Lattice attacks on digital signature schemes. Des. Codes Cryptogr. **23**, 283–290 (2001).
6. LeVeque W.J.: Fundamentals of Number Theory. Addison-Wesley (1977).
7. McCurley K.S.: A key distibution system equivalent to factoring. J. Cryptol. **1**, 95–105 (1988).
8. Menezes A.J., van Oorschot P.C., Vanstone S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton, Florida (1997).
9. National Institute of Standards and Technology (NIST). FIPS Publication 186: Digital Signature Standard. May 1994.
10. Nguyen P., Shparlinski I.E.: The insecurity of the digital signature algorithm with partially known nonces. J. Cryptol. **15**, 151–176 (2002).
11. Saryazdi S.: An extension to ElGamal public key cryptosystem with a new signature scheme. Communication, control, and signal processing, In: Arikan E. (ed.) Proceedings of the 1990 Bilkent International Conference, held at Bilkent University, Ankara, Turkey, 2–5 July 1990. Elsevier (1990).
12. Tan C.H., Yi X., Siew C.K.: Signature Scheme Based on Composite Discrete Logarithm. In: Proceedings of the 2003 Join Conference of the Fourth International Conference on Information, Communications and Signal Processing and the Fourth Pacific Rim Conference on Multimedia, vol. 3, Issue 15–18 Dec. 2003, pp. 1702–1706.