Arab Gulf J.Scient. Res., **12** (1), pp.41 - 53(1994)

Randomized Encryption and Signature Schemes

Nasir A.Al-Darwish

Information and Computer Science Department,
King Fahd University of Petroleum and Minerals,
Dhahran 31261, Saudi Arabia

ABSTRACT. An encryption scheme is randomized if many ciphertexts correspond to a given plaintext. In this paper we propose a simple and effective randomized public key encryption scheme. The scheme is based on the problem of finding a square root modulo n, where n is a product of two large distinct primes. The proposed scheme does not reveal any partial information and breaking it is as hard as factoring n. A randomized public key signature scheme is also proposed.

A cryptosystem protects readable information (plaintext) from unauthorized access by transforming it into unintelligible form (ciphertext). The transformation process is known as encryption. A legitimate user has extra information to help carry out the reverse transformation, known as decryption. The extra information is known as the decryption key. A cryptosystem defines two algorithms, one for encryption (E) and the other for decryption (D). These algorithms use extra parameters known as encryption and decryption keys (k). In other words, a cryptosystem is defined by two mappings, E_k: Messages $\rightarrow$ Ciphertexts and D_k: Ciphertexts $\rightarrow$ Messages. A general cryptosystem is designed with the assumption that the encryption and decryption algorithms as well as the ciphertext are known to outsiders. Thus it is essential that the key space be too large to make exhaustive search for the key infeasible.For a long time cryptosystems were designed with the assumption that both encryption and decryption keys are to be kept secret. These cryptosystems, known as secret-key cryptosystems, do not offer a solution to the problem of a secure transfer of the keys between the sender and receiver in the first place. It was not until 1976 when Diffie and Hellman (Diffie and Hellman 1976) suggested that only the decryption key be made secret, while the encryption key can be made public. Thus the idea of public key cryptosystems was born.

In a public key cryptosystem, each user X maintains two keys; an encryption key (e_X) which is made public and a decryption key (d_X) which is kept secret. The encryption keys for all users are maintained by a trusted authority and published in a public directory, much like a phone directory. A user A wishing to send a message M to another user B looks up the encryption key for B, computes $C = E_B(M)$ and sends C. The user B upon receiving C recovers the original message as $M = D_B(C)$. The notation E_B, D_B means using the encryption key, e_B, and the decryption key, d_B, of user B respectively.

Public key cryptosystems offer many advantages over secret key cryptosystems:

1 - The number of keys required for n users will be 2n keys compared with about n^2 keys in a secret key cryptosystem.
2 - Transfer of the (encryption) key is no problem since it is made public.
3 - In a secret key cryptosystem, the knowledge of (plaintext, ciphertext) pairs usually enable an attacker to discover the key. Thus to make these systems secure it is essential that the key size be large for large messages and that it is changed often. On the other hand, a public key cryptosystem is secure against this type of attack and the key size is independent of the message size and rarely needs to be changed.

Despite their advantages, none of the public key cryptosystems proposed thus far, can compete in speed with commonly known secret key cryptosystems such as Data Encryption Standard (National Bureau of Standards 1977). Though no practical cryptosystem (public key or otherwise) is proven to be unbreakable, breaking some public key cryptosystems has been proven to be equivalent to solving some known difficult problems.

Mathematical Background

Given some fixed positive integer n, any integer x can be written as $x = q \times n + r$, where q and r are integers and $0 \leq r < n$. Here r is the remainder when dividing x by n. This remainder is referred to as x mod n.

Addition (multiplication) of numbers modulo n is same as ordinary addition (multiplication) except that the result is reduced modulo n. For any integer x, the additive inverse of x mod n, denoted by -x mod n, is defined such that $x + (-x) \bmod n = 0$. The multiplicative inverse of x mod n, denoted by $x^{-1} \bmod n$, is defined such that $xx^{-1} \bmod n = 1$ (usually $x \times y$ is written as xy). Clearly the additive inverse of x mod n is n-x. The multiplicative inverse of x mod n exists only if gcd (x,n) =1, where gcd(x,n) denotes the greatest common divisor of x and n, and it can be found using the

Euclid's gcd algorithm. This algorithm also enables the determination of integers a and such that gcd(x,n) = ax + bn. Thus x^{-1} mod n= a mod n.

Let P be a prime number. A positive integer a < p is a *quadratic residue modulo p* if there exists some positive integer x < p such that x^2 mod p = a, otherwise, a is a *quadratic nonresidue*. For example, 2 is a quadratic residue modulo 7 since 4^2 mod 7=2. Thus the quadratic residues modulo p is the set $\{1^2 \bmod P, 2^2 \bmod p, \ldots, (p-1)^2 \bmod p\}$. As it turns out the set contains (P-1)/2, assuming that p is an odd prime, distinct elements. The equation (in the unknown x) x^2 mod p=a where p is an odd prime and a is a quadratic residue, modulo, has two distinct integer (modulo p) solutions of the form x, p-x. If a is not a quadratic residue modulo p then the equation has no integer solutions.

The definition of a quadratic residue is generalized by allowing the modulus to be any positive integer n but restricting x in the above definition to be relatively prime with n (*i.e.* gcd (x,n)=1). For example, 4 is a quadratic residue modulo 21 since 16^2 mod 21=4 and gcd (16,21)=1. If the modulo n is a product of two distinct odd primes p and q then ϕ (n)= (P-1) (q-1) and one quarter of these are quadratic residues modulo n, where ϕ (n) counts the number of elements in the set { 1,2,...,n-1} that are relatively prime with n. For example, the set of quadratic residues modulo 15 contains (2×4)/4= 2 elements, namely 1 and 4. The equation in the unknown x, x^2 mod n =a where n is a product of two distinct odd primes and a is some known quadratic residue modulo n has four distinct integer (modulo n) solutions of the form x,n-x, y and n-y and exactly one of these is a quadratic residue modulo n. If a is not a quadratic residue then the equation has no integer solution. The solutions to the equation, thanks to the Chinese Remainder Theorem, are given by the expression$(w_1 x_1 + w_2 x_2)$ mod n, where $w_1 = q\,(q^{-1} \bmod p)$, $w_2 = p\,(p^{-1} \bmod q)$, x is either x_1 or $(p-x_1)$, and y is either x_2 or $(q-x_2)$ where x_1 and x_2 are the solutions to the equations x^2 mod p = a and x^2 mod q = a respectively. Solving these last two equations is particularly easy when p mod 4 =q mod 4=3 and the solution is given by the formula $x_1 = a^{(p+1)/4}$ mod p and $x_2 = a^{(q+1)/4}$ mod q. As an example, to find the solutions to x^2 mod 21 = 4, we compute $x_1 = 4^{(3+1)/4}$. mod 3 = 1 and $x_2 = 4^{(7+1)/4}$ mod 7 =2. We also compute w_1 = $7\,(7^{-1} \bmod 3) = 7$, $w_2 = 3\,(3^{-1} \bmod 7) = 15$. Thus we obtain (7×1 + 15 ×2) mod 21= 16, (7×2 + 15×2) mod 21 =2, (7×1 + 15×5) mod 21= 19 and (7 × 2 + 15 × 5) mod 21 = 5.

If n is a product of two odd primes p and q, then the factors p and q can be easily found if two independent solutions x and y are known for any quadratic equation x^2 = a mod n. As a matter of fact some factoring algorithms are based on this (Pomerance 1984). It can be shown that gcd(x + y,n) is either p or q and gcd(x-y,n) is either p or q.

A notion relevant to the design of public key cryptosystems is the concept of a one way function and a trapdoor one way function. A function f is a one way function, if for almost all points x in its domain,the computation of f(x) given x is easy but given f(x) the determination of x is generally difficult. Here easy means requiring short computer time (*i.e.* minutes or hours) and difficult means requiring very long (*i.e.* hundreds of years) computer time. If, on the other hand, x can be determined easily from f (x) only when some secret (trapdoor) information is known and generally remains difficult to find even when the algorithm for computing f(x) is made public, then f is a trapdoor one way function.

Squaring modulo n, where n is a product of two odd primes p and q, where p mod 4 = q mod 4 =3 is a trapdoor one way function, since squaring modulo n is easy but finding square root is difficult unless the factorization of n (trapdoor) is known. In general,the problem of finding x such that $x^a = b \bmod n$ (here a, b and n are all fixed positive integers) can be solved easily if the factorization of n is known. Thus $f(x) = x^a \bmod n$ is believed to be a trapdoor one way function. On the other hand, consider the problem of finding x such that $a^x = b \bmod n$. This is known as the discrete logarithm problem for which there is no known trapdoor. Thus it is believed that $f(x) = a^x \bmod n$ is a one way function. Computing f(x) by repeated squaring requires on the order of log(x) (*i.e.* $\leq \log(n)$) multiplication operations whereas the fastest known algorithm for computing the inverse of f(x) requires on the order of $\sqrt{n}$ multiplication operations. Another example of a candidate one way function is integer multiplication. It is easy to multiply very large integers whereas there is no known efficient algorithm for factoring a very large integer. On the other hand, it is never proven that such an algorithm does not exist. Thus it is still open whether integer multiplication is indeed a one way function or not.

Rabin's Public Key Cryptosystem

The problem of factoring a large integer is the basis for the now famous RSA public key cryptosystem (Rivest and Adleman 1978). A variation of this cryptosystem was proposed by Rabin (Rabin 1979). Rabin's scheme is simpler and more efficient than RSA and breaking it is easily proven to be equivalent to factoring (breaking RSA is conjectured to be equivalent to factoring).

In Rabin's scheme each user selects two large primes p and q where p mod 4 = q mod 4=3, and publishes $n = p \times q$ as his public key and keeps p and q secret. To send a message M (assumed to be a large positive integer and gcd(M,n) = 1), to a user whose public key is n, the message is encrypted as $C = M^2 \bmod n$. Upon receiving C, the quadratic equation (in the unknown x) $x^2 = C \bmod n$ is solved using a simple formula in terms of p and q as explained in the previous section. Breaking Rabin's encryption scheme system easily shown to be equivalent to factoring the encryption modulus, n.

Rabin's scheme has a minor problem, namely that there is 4 : 1 ambiguity about the original message that was sent. Williams (Williams 1980) proposed a modification to Rabin's system to remove this ambiguity.

Randomized Encryption

Randomized encryption schemes are those schemes in which more than one ciphertext correspond to a plaintext. These shemes are considered semantically secure, *i.e.* schemes that ensure the secrecy of all partial information about transmitted messages.

In the secret-key cryptosystems randomized encryption is exemplified by homophonic substitution. In a homophonic substitution cryptosystem a message M consisting of a string from an alphabet A_1 is encrypted into a random ciphertext C of symbols from an alphabet A_2, where $|A_2| > |A_1|$. If A_1 has t symbols then A_2 is partitioned into disjoint non empty subsets S_i's ($1 \leq i \leq t$) so that symbol s_j from A_1 is encrypted into a random element of the subset S_j.The key is the partition $(S_1,S_2...S_t)$.

ElGamal (ElGamal 1985) proposed a randomized public key cryptosystem based on the discrete logarithm problem. In this system, all users of the system are informed of a large prime p together with a primitive root g modulo p (*i.e.* Powers of g modulo p generate all the elements$\{1,2,...,p-1\}$). The private key of a user is an integer d chosen at random by the user where $1<d<p$ and the corresponding public key $e= g^d \bmod p$.

In order to send a message M to a user with public key e, the sender chooses a random integer $r, 1 < r < p$ and computes $K = e^r \bmod p$ and sends the pair (C_1,C_2) where $C_1=g^r \bmod p$ and $C_2 = KM \bmod p$.

The receiver first recovers K from C_1 as $K = C_1^d \bmod p$. This follows since $K= e^r \bmod p= (g^d)^r \bmod p = (g^r)^d \bmod p. = C_1^d \bmod p$. Then the receiver recovers M form C_2 as $M= C_2(k^{-1} \bmod p) \bmod p$.

One difficulty with ElGamal's cryptosystem is that of finding a primitve root modulo a very large prime p. Our proposed cryptosystem does not have this kind of problem. The proposed cryptosystem can be looked at as introducing randomization in Rabin's scheme. The underlying theory of quadratic residues has been used as a basis for building a pseudo-random sequence generator used in a public key encryption scheme (Brassard 1988, Blum *et al.* 1986).

Proposed Encryption Scheme

In this cryptosystem each user selects as his public key an integer (n) whcih is a product of two large distinct primes (around 100 decimal digits each) p and q where p mod 4=q mod 4=3. The user also computes and keeps secret the values $w_1 = q\ (q^{-1} \bmod p) \bmod n$, and $w_2 = p\ (p^{-1} \bmod q) \bmod n$. The message space is the set of positive integers $> n$.

To send a message M to a user whose public key is n, the sender selects at random a quadratic residue r mod n (to do this, let $r = r'^2$ where r' is a randomly chosen integer in $\{2,\ldots,n\}$ and gcd $(r',n) = 1$), and sends the pair (C_1, C_2), where $C_1 = r^2 \bmod n$, and $C_2 = M+r \bmod n$. The receiver first recovers r as $r = (w_1 x_1 + w_2 x_2) \bmod n$, where $x_1 = C_1^{(p+1)/4} \bmod p$ and $x_2 = C_1^{(q+1)/4} \bmod q$. Then he recovers M as $M = (C_2 - r) \bmod n$.

Note that for any x, x is a quadratic residue modulo n if and only if x is a quadratic residue modulo p and modulo q. Thus since C_1 is a quadratic residue modulo n, it is a quadratic residue modulo p (q). Also x_1 (x_2), being a product of quadratic residues, is a quadratic residue modulo p (q). But the expession used by receiver for r evaluates to a quadratic residue modulo p and modulo q since it evaluates to x_1 modulo p and x_2 modulo q. Thus the expression for r gives the *quadratic* residue solution modulo n.

Example:

Suppose a user A has selected p=7 and q = 11. Thus n = 77, $w_1 = 11\ (11^{-1} \bmod 7) \bmod 77 = 22$, and $w_2 = 7(7^{-1} \bmod 11) \bmod 77 = 56$.

A user B who likes to send a message M =10 to A, would, say, select r'=3. Thus $r = r'^2 \bmod 77 = 9$ and $r^2 \bmod 77 = 4$. He then would send the pair (4,19).

The receiver Acalculates $x_1 = 4^{(7+1)/4} \bmod 7 = 9$ and $x_2 = 4^{(11+1)/4} \bmod 11 = 9$. Then he computes $r = (w_1 x_1 + w_2 x_2) \bmod n = (22.9+56.9) \bmod 77 = 9$, and recovers $M = (19-9) \bmod 77 = 10$.

In this scheme, the sender should ensure that $r^2 > n$; otherwise, r can be recovered by an attacker by taking ordinary square root. This is not much of a restriction since the range that is excluded for the choice of r is $[1,\sqrt{n}]$ which accounts for a proportion of $\sqrt{n}/n = 1/\sqrt{n}$. But this proportion decreases as n increases and for n being about 200 decimal digits this proportion is quite negligible. On the other hand, the proposed scheme has several desirable properties. The message M can be freely chosen as any positive integer $< n$ and short messages need not be padded. Also there is no ambiguity in the decryption process. Overall, the proposed scheme offers some important benefits over Rabin's at the expense of some data expansion (doubling the

amount of the information sent) -- unavoidable cost with randomized encryption (Brassard 1988). Though the sender does two squaring operations, this cost is somewhat offset by the fact that the receiver does not need to find more than one solution for the quadratic equation. The test for $gcd(r^1,n)=1$ need not be implemented since out of the values $\{1,2,...n-1\}$ only a very negligible proportion $(=(p+q)/pq)$ fails this test.

Signing Messages

The purpose of signing a message is two-fold, to assure the receiver of the identity of the sender (sender authenticity) and of the message integrity (message authenticity). A message is authentic if it has not undergone any tampering or distortion after it was signed. Both of these independent requirements can be met by a process known as *digital signature*.Like a hand-written signature (or a fingerprint), a digital signature provides some undeniable and unforgeable link to its originator. However, unlike a hand-written signature, a digital signature is message dependent; otherwise it can be cut and pasted to other messages. Several digital signature schemes are described in Seberry and Pieprzyk (1989). A proposal for a digital signature standard is discussed in (Rivest *et al.* 1992).

Let m denote the number of quadratic residues mod n where n is a product of two large primes p and q (*i.e.* $m= (p-1)(q-1)/4$). Since the set of quadratic residues mod n is a *group* under multiplication mod n, it follows that for any quadratic residue x, $x^m \bmod n = 1$ This implies that $x^k \bmod n = x^{k \bmod m} \bmod n$. To sign a message M by a sender whose modulo is n, the sender selects at random a positive integer r such that $gcd(r,m)= 1$ and calculates $s=r^{-1} \bmod m$ and $C = (M^2)^r \bmod n$. He then sends the triple (M,C,s). Here the pair (C,s) is a message authenticator since it is determined from M and the message originator knowledge of the factorization of n. The receiver accepts M as authentic if $M^2 \bmod n = C^s \bmod n$.

A signature scheme is secure if it does not allow an attacker to find the user's private information or to sign arbitrary messages on the user's behalf. If an attacker recovers r then he will be able to sign new messages using r and s. However, it is not easy to recover r from C since this corresponds to solving an instance of the discrete logarithm problem. But then the determination of m from s and n seems impossible. As a matter of fact the determination of m is equivalent to factoring n, since $m = \varnothing(n)/4$ and the knowledge of $\varnothing(n)$ enables the computation of p and q using the following equations.

$$p + q = n - \varnothing(n) + 1 \qquad (1)$$

$$p - q = ((p + q)^2 - 4n)^{1/2} \qquad (2)$$

It is very unlikely that the message M can be tampered with in a meaningful way and still satisfy this test. One possible tampering is to transform (M, C,s) into (M^k mod n, C^k mod n, s) for an arbitrary integer k. However this approach does not enable an attacker to sign an arbitrary message $M^1=M^k$ mod n, since this corresponds to solving an instance of the discrete logarithm problem. As noted by ElGamal (ElGamal 1985), this problem is present in all existing digital signature schemes. This problem is solved by imposing some structure on valid messages *(e.g.*A message is some English text) so that the preceding attack is very unlikely to result in a message with a valid structure.

In ElGamal's scheme, the message authenticator gives rise to a linear equation in three variables: the message, the user's private information, and a random value. If the same random value is used to sign two different messages, then one gets two linear equations in two unknowns, the random value and the user's private information, and therefore is able to discover the user's private information.

Note that the roles of s and r in the above scheme are interchangeable. Thus the sender can select s to be a small number to make the verification procedure time efficient. Selecting s to be small also means that the signature itself is about the same size as the message. It is advisable that r should be large enough so that its recovery by exhaustive search is infeasible.

The signing procedure can be made more efficient by not changing r so often.This may not compromise the scheme, since in this way the scheme can be thought of as a variation of the RSA-based signature scheme. In RSA r and s are selected to be such that rs = 1 mod $\varnothing$(n) (rather than rs=1 mod $\varnothing$(n)/4). If we vary s with each message (in RSA s is fixed and is part of the public key) then the authenticator of a message M is simply ($C=M^r$ mod n, s) and the message M can be any value such that gcd (M,n) which is almost always guaranteed. In this case, assuming the message has a certain structure, the message itself need not be sent. The receiver recovers M as C^s mod n and accepts it as authentic if it has a valid structure.

Securing and Signing Messages

In certain applications, like the signing of a public contract, a signed message need not be encrypted. If the message is to be both signed and made secure then the above schemes of securing and signing a message can be combined. This can be done by one of two methods, depending on the order of applying sign and secure operations. To illustrate this, assume that a sender A with public key n_A is to send a secure and signed message to a receiver B with a public key n_B.

1. (Sign then secure) The sender A with some message M computes (C,s) which is an authenticator for M. He also selects at random a quadratic residue r mod n_B. He then sends (M+r mod n_B, r^2 mod n_B, C,s). The receiver B first finds r from the second component and M from the first component. Then he verifies that M is authentic and originated from A by verifying that M^2 mod $n_A=(C)^s$ mod n_A.

2. (Secure then sign) The sender A with a message M selects at random a quadratic residue r mod n_B and computes C=M+r mod n_B. He also computes (C',s) which is an authenticator for C based on a different random number other than r. He then sends (C, r^2 mod n_B, C',s). The receiver B first verifies that C is authentic and originated from A by verifying that C^2 mod $n_A=(C')^s$ mod n_A. He then finds r from the second component and M from the first component.

This latter method has a strange property in that it allows a third party to verify the signature of a message without being able to read the actual message.

User Identification

The password based user identification scheme commonly used to identify users in a computer system is vulnerable to a replay attack. An eavesdropper who is a able to intercept some one's else password can use it to enter into the system. A neat solution to this problem is provided by using a public key cryptosystem. Each user registers his pupblic key encryption scheme with the system. Whenever a user logins to the system, the system generates a random message M, and lets C=E(M). The system sends C to the user which in turn replies with D(C). The user is allowed to use the system only if the reply is M. It does an impersonator no good to monitor an exchange between a user and the system since he is likely to face a different challenge when he tries to login into the system. Alternatively a signature scheme can be employed as a basis for a user identification scheme by challenging the user to produce a valid signature for an arbitrarily chosen message.

In either scheme there must be an assurance to the user that the above interaction does not help the system in figuring out the user's private information. As noted by Brassard (Brassard 1988), the encryption scheme should resist chosen-ciphertext attack, in which an attacker (system) gives the user an encrypted text and asks for the corresponding plaintext. Consider the situation where the proposed encryption scheme is used but the system cheats and sends (r^2 mod n, C=M+r mod n), where r is a quadratic nonresidue mod n instead of r being a quadratic residue as demanded by the encryption scheme. Then from the user's reply which is C-r the system will figure out the other independent solution r' to the quadratic equation and thus be able to factor n.

On the other hand, consider the situation where the proposed signature scheme is employed. Having seen one signature (M, M^r mod n, s) for a message M, the attacker might ask for a signature to another message M^1 and gets (M^1, $M^1 r^1$ mod n, s^1). Even if $M^1$is chosen to have a link to the user's private information (*e.g.*$M^1 = M^s$ mod n), the user is free in his choice of r^1 and s^1 and it is not clear if the signature for M^1 will be of any help in figuring out some useful information about the user's private information such as knowing r or r^1. Unlike the encryption scheme, the signature scheme leaves the randomization element in the user's hand. For further information about authentication in computer systems refer to (Woo and Lam 1992).

Concluding Remarks

We proposed some new encryption and signature schemes. The security of these schemes is based on the supposed difficulty of factoring. The encryption and signature schemes overcome certain problems present in similar past schemes. The proposed schemes are efficient in terms of the processing required and the amount of data that has to be communicated.

References

Blum, L., Blum, M. and **Shub, M.** (1986) A simple unpredictable pseudo-random number generator, *SIAM Journal on Computing*, **15:** 364-383.

Brassard, G. (1988) *Modern Cryptology*, Lecture Notes in Computer Science # 325, Springer-Verlag.

Denning, D.R. (1982) *Cryptography and Data Security*, Addison-Wesley.

Diffie, W. and **Hellman, M.** (1976) New Directions in Cryptography, *IEEE Tran. Info. Theory*, **22**(IT): 644-654.

ElGamal, T. (1985) A public key cryptosystem and a signature scheme based on discrete logarithm, *IEEE Tran. Info. Theory*, **31**(IT): 469-472.

National Bureau of Standards (1977) *Report of the Workshop on Cryptography in Support of Computer Security*, NBSIR 77-1291, Sep. 1977.

Pomerance, C. (1984) Lecture Notes on Primality Testing and Factoring, *Mathematical Association of America* (MMA) Notes, no. 4.

Rabin, O. (1979) *Digitalized signatures and public-key functions as intractable as factorization*, Technical Report, MIT/LCS/TR212, MIT Lab. Computer Science, Cambridge, Mass. Jan. 1979.

Rivest, S. and **Adleman,** (1978) A method for obtaining digital signatures and public key cryptosystems, *CACM, Feb. 1978* **21**(2)**:** 120-128.

Rivest, R. (1978) Remarks on a proposed cryptanalytic attack on MIT public key cryptosystems, *Cryptologia*, **2**: 62-65.

Rivest, H. and **Anderson, L.** (1992) Responses to NIST's Proposal, *Communications of the ACM*, **35**(7)**:** 41-45.

Seberry, and **Pieprzyk,** (1989) *Cryptography: An Introduction to Computer Security*, Prentice-Hall.

Williams, H. (1980) A modification of the RSA public-key encryption procedure, *IEEE Tran. Info. Theory,* **26**(IT): 726-729.

Woo, T. and **Lam, S.** (1992) Authentication for Distributed Systems, *IEEE Computer.* **25**(1): 39-52.

Yao, A. (1982) Theory and applicaions of trapdoor one way functions, *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science,* pp. 80-91.

(Received 24/02/1993;
in revised form 20/06/1993)

طرق التعمية والتوقيع العشوائية

ناصر علي آل درويش

قسم علوم الحاسب والمعلومات ـ جامعة الملك فهد للبترول والمعادن
الظهران ٣١٢٦١ ـ المملكة العربية السعودية

إن أي نظام للتعمية يوفر طريقة رياضية لتحويل النص الواضح (المقروء) إلى نص مُعمَّى (غير مقروء) وهناك طريقة مغايرة يتم بواسطتها تحويل النص المُعمَّى إلى نص واضح وتستند كل من الطريقتين إلى قيمة معينة تعرف بمفتاح التعمية ومفتاح فك التعمية على الترتيب. ويكون الهدف من نظام التعمية أنه حتى مع معرفة طريقة التعمية لا يمكن فك التعمية دون معرفة مفتاح فك التعمية. كذلك فإن أي نظام عملي للتعمية يجب أن يوفر عدداً كبيراً جداً من المفاتيح حتى لا يمكن معرفة النص المُعمَّى عن طريق تخمين مفتاح فك التعمية.

هذا وقد ظلَّ علم التعمية لفترة طويلة يفترض ضمان سرية مفتاح التعمية ومفتاح فك التعمية، إلا أن ذلك تغير عام ١٩٧٦م عندما أقترح ديفي و هلمان أن يكون مفتاح التعمية مُشاعاً (عمومياً) بينما يبقى مفتاح فك التعمية سرياً.

وبذلك وُلدت أنظمة التعمية الحديثة ذات المفاتيح العمومية والتي كان من أشهرها نظام آر أس أ (RSA) الذي ظهر في عام ١٩٧٨م. وقد أجتذبت هذه الأنظمة إهتمام الكثير من الباحثين لما لها من ميزات خاصة وتطبيقات عديدة

نـذكر بعضهـا في هذا البحث. وتكـون طريقـة التعميـة عشـوائيـة إذا كـان من خاصيتها تحويل النص الواضح إلى أكثر من نص مُعمَّى.

وفي هذا البحث نُقدم طريقة عشـوائية بسيـطة وفعالـة للتعمية ذات مفتـاح عمومي. وتعتمد هذه الطريقة على مسألة إيجاد الجذر التربيعي مدى ن حيث أن ن هي حـاصل ضـرب عددين أوليـين مختلفين وكبيـرين. إن الطريقـة المقترحـة لا تكشف أي معلومة جزئيـة كما أن كسـرها مـماثل لصعـوبة تحليـل ن. كذلـك يتضمن البحث طريقة توقيع عشوائية ذات مفتاح عمومي.