|  |
| --- |
| **Executive Summary** |
|  |
| P.3.4 Assignment – RSA  SPRINT 03  Cyber Infrastructure Design & Strategy |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **What is trapdoor function?**  a function defined from data by means of a mathematical procedure in such a way that it is easy to obtain the function when the data are known, but when the procedure and data are not known it becomes very difficult to determine the original data: used in cryptography, where the data are the characters of the plain text, or message, and the trapdoor function is the cryptogram.  Trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction (finding its inverse) without special information, called the "trapdoor". Trapdoor functions are a special case of one-way functions and are widely used in public-key cryptography.[2]  Informally, a function f:{0,1}^(l(n))×{0,1}^n->{0,1}^(m(n)) is a trapdoor one-way function if  1. It is a one-way function, and  2. For fixed public key y in {0,1}^(l(n)), f(x,y) is viewed as a function f\_y(x) of x that maps n bits to m(n) bits. Then there is an efficient algorithm that, on input <y,f\_y(x),z> produces x^' such that f\_y(x^')=f\_y(x), for some trapdoor key z in {0,1}^(k(n)).  f is a trapdoor one-way hash function if f is also a one-way hash function, i.e., if additionally  3. Given M and f(M), it is hard to find a message M^'!=M such that f(M^')=f(M).    **Basic trapdoor function**   |  |  |  | | --- | --- | --- | | **1093\*1039** | **=** | **1,135,627** | | **Two prime numbers** | **Factorization by 15** | **5,3** |   **What is RSA?**  It is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977.  In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.    Example:  First, let’s assume you calculated your keys as follows:  p=17 and q =7. Notice 17 and 7 are both prime numbers  n= 17 x 7 = 119  f(n) = (17-1)(7-1)=96  e=11, notice that gcd(96,11)=1 and 1<11<96  d=35  The keys are:  private key: {35,96}  public key: {11,96}  Now, you published somehow your public key and I want to send you a message only can read.  The message I want to send you is M=21. Notice that you can always find a numeric representation for any message. At the end of the day, all data in a computer is represented as numbers.  C = Me mod n=2111 mod 96 = 45  When you receive the encrypted message C=45, you use your private key to decrypt it.  M = Cd mod n=4535 mod 96 = 21  **What is Bellcore attack?**  Bellcore attack is a well-known fault attack that is able to break RSA and the variant RSA-CRT.  RSA-CRT transforms message m into signature s using private key p, q, dp, dq as follows:  sp = ( mp )dp mod p,  sq = ( mq )dq mod q,  s = ( ( (sq – sp) · pinv) mod q) · p + sp,  where mp = m mod p, mq = m mod q, pinv= p–1 mod q.  Suppose either sp or sq is computed with a fault. Assume that the resulting faulty signature s' together with the correct signature s are known to the attacker. Then he can retrieve the private key by computing:  gcd(s – s', N)  for the publicly known RSA modulus N. Alternatively, the attacker can recover the private key from s' and m by computing:  gcd(m – ( ( s' )e mod N ), N),  **References**  https://en.wikipedia.org/wiki/Trapdoor\_function  <https://mathworld.wolfram.com/TrapdoorOne-WayFunction.html>  <https://justcryptography.com/rsa-algorithm/>  <https://eprint.iacr.org/2012/553.pdf> |  |  |