CO3326 Computer Security: Coursework Assignment Report

Introduction

Cryptographically secure pseudorandom number generators (CSPRNGs) are important for cryptographic systems as they guarantee data encryption's security and integrity. One of the most investigated CSPRNGs within the cryptography community is the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG), due to its integrity concerns and potential vulnerabilities. This report focuses on the Dual_EC_DRBG, elliptic curve cryptography (ECC), and the discrete logarithm problem's theoretical foundations, answering specific questions under these sections.

Question 1: Elliptic Curve Discrete Logarithm Problem (ECDLP)

The elliptic curve discrete logarithm problem (ECDLP) serves as the basis for the security of ECC-based cryptographic systems. It involves finding an integer k such that Q = kP given two points P and Q on an elliptic curve, where P and Q are points on the curve and k is a scalar. The security of ECC depends on the difficulty of solving ECDLP with respect to being unable to compute k given the current computational power.

Question 2: Analysis of a Given Elliptic Curve

The given elliptic curve E: $y^2 = x^3 - 3x + 2$ over the real numbers R is not singular because its discriminant $\Delta = -16(4(-3)^3 + 27(2)^2)$ is non-zero. Nonzero discriminates signifies that the curve does not have any cusps or self-intersections which are characteristics of singular curves. For cryptographic purposes, it is essential to use non-singular curves since singular curves do not provide the necessary group properties and security assumptions required for ECC.

Question 3: The Implications of Using Singular Elliptic Curves

Employing singular elliptic curves does not support an abelian group that is a condition for ECC system together with abelian groups. In other words, singular curves are improper in use of this structure not only because they are not well-defined. In the presence of cusp or self-intersection on singular curve, the group operation is not clear and meaningful, thereby getting out of the field of ECC. In the cryptography scheme, providing security and predictable is essential, singularity led to unpredictable outcomes, those implications are dangerous to develop ECC's secure system. Moreover, because singular curves allow to reduce ECDLP's complexity, therefore it significantly effects on cryptoanalysis's result.

Question 4: Elliptic Curve Operations Over Finite Field F_{43}

i. Perfect Squares in F_{43}

To determine for which values of x in F_{43}, $x^3 + 7$ is a perfect square, one must evaluate $x^3 + 7$ for each x in F_{43} and check if the result is a quadratic residue modulo 43. This process involves computing the Legendre symbol for each possible outcome.

ii. Point Addition

The addition of points (13, 22) and (21, 25) on the curve E: $y^2 = x^3 + 7$ over F_{43} follows the elliptic curve group law. The slope s of the line connecting the points is calculated first, followed by the determination of the resulting point's coordinates using the formulas for elliptic curve addition.

iii. Scalar Multiplication Examples

Scalar multiplication, such as 17·(13,21)17·(13,21) and 31·(12,12)31·(12,12), involves repeatedly adding a point to itself on the elliptic curve. The process for these specific examples highlights the cyclic nature of elliptic curve points over finite fields and demonstrates the computational aspect of ECDLP.

iv. Significance of Scalar Multiplication

The result of scalar multiplication, especially in cases like 31·(12,12)31·(12,12), illustrates the concept of point doubling and the efficient computation methods available for elliptic curves, such as the double-and-add algorithm.

v. List all points on E, i.e., list E(F_{43}).

To list all points on E: $y^2 = x^3 + 7$ over F43, one calculates the right-hand side of the curve equation for each x in F43 and checks if the result is a square in F43. A point (x, y) is on the curve if there exists a y such that $y^2 \equiv x^3 + 7$ (mod 43). The point at infinity, denoted as O, is also included as it serves as the identity element in the elliptic curve group.

vi. What is the order of the curve? What is the cofactor? Explain why.

The order of an elliptic curve, denoted as #E(F43), is the total number of points on the curve, including the point at infinity. The cofactor, h, is defined in relation to the prime order n of a subgroup of the curve and the curve's total order, such that #E(F43) = h × n. Determining the order of the curve involves counting all valid points (including O), while the cofactor reflects the multiplicity of the subgroup order to reach the total curve order. For cryptographic applications, a small cofactor (preferably h = 1) is desired to maximize the security provided by the curve.

Question 5: Criticisms of Dual_EC_DRBG

In addition to the NSA alleged backdoor, Dual_EC_DRBG was criticized for its inefficiency and the possibility of biases in the output sequence. The use of ECC by the generator made it significantly slower than other CSPRNGs. On the design side, the structure of the algorithm allowed for the manipulation of the output and hence raised questions regarding the suitability of this PRNG in demanding cryptographic applications.

Question 6: Reversing the Truncation to Find *x*

Finding x by inversing the truncation is critical to investigate the potential vulnerability of Dual_EC_DRBG. Truncation is to strip off the low-order bits of the output to strengthen the security of the PRNG by concealing the internal state sk as much as possible. On the condition for reversing truncation, or essentially guessing the low-order bits, the breach of randomness will be irretrievable. Inversing the operation of truncation is equivalent to either estimating the low-order bits or utilizing side-channel information to restore those bits. Although achievable in theory, it is computationally expensive and demanding to expose more knowledge, such as the internal state or the structure of the algorithm, to facilitate the estimate of low-order bits exclusively.

Question 7: The Factor as a Backdoor

The given factor for this assignment, akin to the NSA's alleged Dual_EC_DRBG backdoor, appears to represent a hidden value that helps guess upcoming pseudorandom numbers produced by the algorithm. The backdoor works by taking advantage of the elliptic curve's mathematical nature, specifically the link between the point pairs P and Q along with their scalar multiples. Observing P and Q values after–the–fact, if an attacker is aware of the backdoor factor's role in P’s relation to Q, this adversary can predict future values produced by the generator after enough generated values have been seen. This ability fundamentally destroys the CSPRNG's security, because it allows an entity aware of the backdoor to foretell future outputs, a breach of a secure pseudorandom number generators unpredictability requirement.

Question 8: Computing the Next Pseudorandom Number Using the Backdoor

The process to compute the next pseudorandom number by the backdoor requires multiple steps that exploit the mathematical properties of elliptic curves and the specific instantiation of Dual_EC_DRBG. Given two consecutive numbers intercepted, the backdoor factor can be employed to extract the internal state of the generator. This process typically entails inversion of the generator's output, to determine the state that would have produced the observed outputs. With the knowledge of the internal state, it can be advanced according to the generator's algorithm. The subsequent output can be predicted. Outlining this procedure demonstrates the practical exploitation of the backdoor. It emphasizes the importance of secure design principles in cryptographic algorithms in order to defend against such weaknesses.

Question 9: Implications of Predicting Pseudorandom Numbers

If the next pseudorandom number generated by Dual_EC_DRBG is predictable, its usage will have serious security implications. It will compromise the confidentiality and integrity of cryptographic systems that rely on this generator for key generation, secure communication protocols, or any application which security requires unpredictability. For example, if an encryption system’s keys can be predicted, it will be possible for an attacker to decrypt sensitive information; or an attacker will be able to impersonate legitimate parties in secure communications. This vulnerability provides a powerful reminder of the absolute necessity of rigorous security evaluations of cryptographic algorithms, and the extremities that can come from vulnerabilities, or hidden badness, whether intentional or unintentional.

Question 10: Design and Implementation of Code

The code design for this assignment was aimed at the faithful implementation of the Dual_EC_DRBG algorithm with an embedded backdoor utilizing the concepts of elliptic curve cryptography. The core of elliptic curve algorithms is the scalar multiplication operation which was implemented using the double-and-add algorithm to improve efficiency. The generation of the next pseudorandom number given the two previous ones involves the integration of the backdoor mechanism by exploiting the feature of the elliptic curve points P and Q.

References

1. Boneh, D. and Shoup, V., 2020. A graduate course in applied cryptography. *Draft 0.5*.
2. Hankerson, D. and Menezes, A., 2021. Elliptic curve cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1-2). Berlin, Heidelberg: Springer Berlin Heidelberg.
3. Koblitz, N., 1994. *A course in number theory and cryptography* (Vol. 114). Springer Science & Business Media.
4. PUB, F., 2000. Digital signature standard (DSS). *FIPS PUB*, pp.186-192.
5. Silverman, J.H., 2009. *The arithmetic of elliptic curves* (Vol. 106, pp. xx+-513). New York: Springer.
6. Washington, L.C., 2008. *Elliptic curves: number theory and cryptography*. CRC press.