Cryptography

Problem set 7 - 23-24 IV 2015

Definition 1. (Blum integer) $N = pq$ is *Blum integer* if p, q are distinct primes with $p = q = 3 \bmod 4$.

1. Find a sequence $(a_i)_{i \geq 1}$ of natural numbers, for which Euclid's algorithm takes exactly i steps to compute $\gcd(a_{i+1}, a_i)$.
2. Let $n = 122351821$ be a Rabin modulus and let $c = 67625338$ be a ciphertext that is obtained by Rabin encryption using this modulus. Determine all possible plaintexts.
3. Consider a "textbook Rabin" encryption scheme in which a message $m \in \mathcal{QR}_N$ is encrypted relative to a public key N (where N is a Blum integer) by computing the ciphertext $c = [m^2 \bmod N]$. Show a chosen-ciphertext attack on this scheme that recovers the entire private key.
4. Explain the low-exponent attack and the multiplicativility attack for the Rabin system. How can those attacks be prevented?
5. Show that a "textbook" RSA encryption scheme is not CCA-secure. Hint: having a ciphertext c show how to select $c' \neq c$ such that knowledge of the corresponding plaintext $x' = \mathsf{Dec}_K(c')$ lets one to find x $(= \mathsf{Dec}_K(c))$.
6. We call a plaintext x a fixed-point for an encryption if $\mathsf{Enc}_K(x) = x$ (for some key). Show that for a "textbook" RSA number of fixed-points $x \in \mathbb{Z}_n^*$ is equal to: $\gcd(e-1, p-1) \cdot \gcd(e-1, q-1)$ (where $n = pq, [N, e]$ - a public key).
7. Let $n = pq$ where p, q are primes. Let $e \in \mathcal{N}$, show that e is prime to $\varphi(n)$ if:

   $$\mu : \mathbb{Z}_n^* \to \mathbb{Z}_n^*, \mu(x) := x^e$$

   is bijective.
8. (2 points) RSA (and Rabin) scheme is insecure if one is able to factor the modulus $n = pq$. It can happen [1] that because of *e.g.,* implementation mistakes two users share the same prime factor *i.e.,* Alice has $n = pq$ while Bob $n' = p'q$ in such a case Eve can find their private keys by just computing $gcd(n, n')$.

   RSA can be implemented in such a way that instead of generating $n = pq$, more primes are used *i.e.,* $n = p_1 \dots p_k$. Lets call such a system $RSA - k$ (where original RSA is $RSA - 2$).

   Given N number of $RSA - k$ keys, each generated from l-bit long primes, find the probability that there exists at least one pair of keys that share the same modulus (answer depends on: N, k, l). Compute exact values for $N = 6 \times 2^20; k = 2, 3, 4, 5; l = 128, 256, 512, 1024, 2028$.
9. Prove that the DDH problem is not hard in $\mathbb{Z}_p^*$. Hint: use the fact that quadratic residuosity can be decided efficiently modulo a prime.
10. Let p be a large prime, such that $q := (p-1)/2$ is also prime. Let $\mathcal{G}$ be a subgroup of order q in $\mathbb{Z}_p^*$. Let g and h be randomly chosen generators in $\mathcal{G}$. We assume that it is infeasible to compute discrete logarithms in $\mathcal{G}$. Show that

    $$f : \{0, \dots, q-1\}^2 \to \mathcal{G}, f(x, y) := g^x h^y$$

    can be used to obtain a collision-resistant compression function.

11. Alice receives the ElGamal ciphertext $c = (30, 7)$, her public key is $(p = 43, g = 3)$. Determine the corresponding plaintext.
12. How can two ElGamal ciphertexts be used to generate a third ElGamal ciphertext of an unknown plaintext? How can this attack be prevented?

References

[1] Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J Alex Halderman. Mining your ps and qs: Detection of widespread weak keys in network devices. In *USENIX Security Symposium*, pages 205–220, 2012.