Cryptography

Problem set 1

1. Find integer numbers X, Y such that $3X + 448Y = 1$.
2. Find a sequence $(a_i)_{i\geq 1}$ of natural numbers for which Euclidean algorithm needs exactly i iterations to find $\gcd(a_{i+1}, a_i)$.
3. Let $x = 130 \in Z^*_{437}$. Use CRT to find a representation of x in $Z^*_{19} \times Z^*_{23}$.
4. Let $p = 23$, $q = 19$ and let $x = (22, 4) \in Z^*_p \times Z^*_q$. What is the value of x in Z^*_{437}?
5. Find $139^{1224} \bmod 1223$.
6. Find $139^{397} \bmod 437$.
7. Prove that if G, H are groups then $G \times H$ is a group.
8. Let $N = pq$ and let $[N, e_1], [N, e_2]$ be public keys of Alice and Bob respectively. Show that if Eve sends encrypted messages to Alice $c_1 = m^{e_1} \bmod N$ and Bob $c_2 = m^{e_2} \bmod N$ and you intercept them then you can recover m from c_1 and c_2. What is the success probability of your attack?.
9. Let $N = pq$ be a product of two distinct primes. Show that if $\varphi(N)$ and N are known, then it is possible to compute p and q in polynomial time.
10. Let $N = pq$ be a product of two distinct primes. Show that if N and an integer d such that $3d = 1 \bmod \varphi(N)$ are known, then it is possible to compute p and q in polynomial time.
11. Let $|N|$ denotes the length of binary representation of N.
    (a) Show that if $N = M^e$ for some integers $M, e > 1$ then $e \leq |N| + 1$.
    (b) Given N and e with $2 \leq e \leq |N| + 1$, show how to determine in *poly*$(|N|)$ time whether there exists an integer M with $N = M^e$.
    (c) Given N, show how to let test in *poly*$(|N|)$ time whether N is a perfect power.
12. Draw the function $f(n) = L_{2^n}[x, y]$ for $n \in \{1, 2, \ldots, 4096\}$ and $(x, y) = (1/2, 1)$, $(x, y) = (1/3, (64/9)^{1/3})$.
13. Factor 11111 using the quadratic sieve.
14. Let $\langle N, e\rangle$ be a public and d a private key of the RSA encryption. You know that $d < \sqrt[4]{N}/3$. Find d. Hints:
    - show that there exists such a k that $ed - k\varphi(N) = 1$.
    - try to approximate $\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{d\varphi(N)}$ with public data and assumptions.
    - use continued fraction to approximate d (k/d).

    You can use the following data to illustrate your algorithm:
    $\langle N, e\rangle = \langle 1335815453373977, 100169346544615\rangle$.

    How to extend the algorithm to the case $d < \sqrt{N}$?
15. 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.

16. Consider the "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.

17. Show that the "textbook" RSA encryption scheme is not CPA-secure.

18. RSA (and Rabin) scheme is insecure if one is able to factor the modulus $n = pq$. It can happen [HDWH12] 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.,* $n = p_1 \ldots p_k$. 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 $N = 6 \times 2^{20}; k = 2, 3, 4, 5; l = 128, 256, 512, 1024, 2028$.

References

[HDWH12] 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.