Midterm #2

MATH 481/581 — Cryptography
Friday, March 29, 2024

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 35 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (3+3 points) Bob's public RSA key is $N = 33$, $e = 13$.

(a) Encrypt the message $m = 5$ and send it to Bob.

(b) Determine Bob's secret private key d.

Problem 2. (4 points) Alice and Bob select $p = 19$ and $g = 15$ for a Diffie–Hellman key exchange. Alice sends 9 to Bob, and Bob sends 12 to Alice. What is their shared secret?

Armin Straub
straub@southalabama.edu

Problem 3. (2+4 points) Consider the finite field $\mathrm{GF}(2^4)$ constructed using x^4+x+1.

(a) Multiply x^2 and x^2+1 in $\mathrm{GF}(2^4)$.

(b) Determine the inverse of x^2 in $\mathrm{GF}(2^4)$.

Problem 4. (4 points) Consider the (silly) block cipher with 3 bit block size and 3 bit key size such that

$$E_k(b_1b_2b_3) = (b_2b_1b_3) \oplus k.$$

Encrypt $m = (100\ 100\ 100\ldots)_2$ using $k = (110)_2$ and CBC mode ($\mathrm{IV} = (111)_2$).

Armin Straub
straub@southalabama.edu

Problem 5. (15 points) Fill in the blanks.

(a) Despite its flaws, it is fine to use the Fermat primality test for $\boxed{}$.

(b) As part of the Miller–Rabin test, it is computed that $26^{147} \equiv 495$, $26^{294} \equiv 1 \pmod{589}$.

What do we conclude? $\boxed{}$

(c) DES has a block size of $\boxed{}$ bits, a key size of $\boxed{}$ bits and consists of $\boxed{}$ rounds.

(d) AES-256 has a block size of $\boxed{}$ bits, a key size of $\boxed{}$ bits and consists of $\boxed{}$ rounds.

(e) Suppose we are using 3DES with key $k = (k_1, k_2, k_3)$, where each k_i is an independent DES key.

Then m is encrypted to $c = \boxed{}$. The effective key size is $\boxed{}$ bits.

(f) Bob's public ElGamal key is (p, g, h). To send m to Bob, we encrypt it as

$c = \boxed{}$. (Indicate if any random choices are involved.)

(g) For his ElGamal key, which of p, g and x must Bob choose randomly? $\boxed{}$

(h) For his RSA key, which of p, q and e must Bob choose randomly? $\boxed{}$

(i) If the public ElGamal key is (p, g, h), then the private key x can be determined by solving

$\boxed{}$.

(j) Which is the only nonlinear layer of AES? $\boxed{}$

(k) For his public RSA key, Bob selected $N = 65$. The smallest choice for e with $e \geqslant 2$ is $\boxed{}$.

(l) For his public ElGamal key, Bob selected $p = 53$. He has $\boxed{}$ choices for g.

(m) 2 is a primitive root modulo 13. For which x is 2^x a primitive root modulo 13? $\boxed{}$

(n) If x has (multiplicative) order N modulo m, then x^{10} has order $\boxed{}$.

(o) The computational Diffie–Hellman problem is: given $\boxed{}$, determine $\boxed{}$.

Armin Straub
straub@southalabama.edu

(extra scratch paper)