Midterm #2

MATH 481/581 — Cryptography
Friday, March 31, 2023

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 32 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 $N = 51$, $e = 13$.

(a) Encrypt the message $m = 7$ for sending it to Bob.

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

Problem 2. (4 points) Alice and Bob select $p = 19$ and $g = 10$ for a Diffie–Hellman key exchange. Alice sends 3 to Bob, and Bob sends 12 to Alice. What is their shared secret?

Armin Straub
straub@southalabama.edu

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

(a) Multiply x^3 and $x+1$ 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

$$E_k(b_1b_2b_3) = (b_1b_3b_2) \oplus k.$$

Encrypt $m = (110\ 110\ 110\ldots)_2$ using $k = (001)_2$ and CBC mode ($\mathrm{IV} = (111)_2$).

Armin Straub
straub@southalabama.edu

Problem 5. (14 points) Fill in the blanks.

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

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

(c) 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.)

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

$\boxed{}$.

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

(f) 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.

(g) AES-128 has a block size of $\boxed{}$ bits, a key size of $\boxed{}$ bits and consists of $\boxed{}$ rounds.

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

(i) For his public ElGamal key, Bob selected $p = 41$. He has $\boxed{}$ choices for g.

(j) For his public RSA key, Bob selected $N = 77$. The smallest choice for e with $e \geqslant 2$ is $\boxed{}$.

(k) 13 is a primitive root modulo 19. For which x is 13^x a primitive root modulo 19?

$\boxed{}$

(l) If x has (multiplicative) order 20 modulo 77, then x^8 has order $\boxed{}$.

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

(n) Up to x, there are roughly $\boxed{}$ many primes.

Armin Straub
straub@southalabama.edu

(extra scratch paper)