Midterm #2

MATH 481/581 — Cryptography
Wednesday, Apr 5

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 36 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (3+3 points) Bob's public ElGamal key is $(p, g, h) = (19, 10, 6)$.

(a) Encrypt the message $m = 5$ ("randomly" choose $y = 2$) and send it to Bob.

(b) Break the cryptosystem and determine Bob's secret key.

Solution.

(a) The ciphertext is $c = (c_1, c_2)$ with $c_1 = g^y \pmod{p}$ and $c_2 = h^y m \pmod{p}$.

Here, $c_1 = 10^2 \equiv 5 \pmod{19}$ and $c_2 = 6^2 \cdot 5 \equiv -2 \cdot 5 \equiv 9 \pmod{19}$. Hence, the ciphertext is $c = (5, 9)$.

(b) We need to solve $10^x \equiv 6 \pmod{19}$. Since we haven't learned a better method, we try $x = 1, 2, 3, \ldots$ until we find the right one: $10^2 \equiv 5$, $10^3 \equiv 12$, $10^4 \equiv 6 \pmod{19}$. Hence, $x = 4$. □

Problem 2. (4 points) You are Eve. Alice and Bob select $p = 41$ and $g = 7$ for a Diffie–Hellman key exchange. Alice sends 15 to Bob, and Bob sends 38 to Alice. What is their shared secret?

Solution. Let's crack Alice's secret y (you can also attack Bob; his is $x = 5$).

For that, we need to find y such that $7^y = 15 \pmod{41}$.

We try all possibilities: $7^2 \equiv 8$, $7^3 \equiv 15 \pmod{41}$

Hence, Alice's secret is $y = 3$. Since $38^3 \equiv (-3)^3 \equiv -27 \equiv 14 \pmod{41}$, the shared secret is 14. □

Armin Straub
straub@southalabama.edu

Problem 3. (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.

Solution.

(a) The ciphertext is $c = m^e \pmod{N}$. Here, $c \equiv 5^{13} \pmod{33}$.

$5^2 = 25 \equiv -8$, $5^4 \equiv 64 \equiv -2$, $5^8 \equiv 4 \pmod{33}$. Hence, $5^{13} = 5^8 \cdot 5^4 \cdot 5 \equiv 4 \cdot (-2) \cdot 5 \equiv 26 \pmod{33}$. Hence, $c = 26$.

(b) $N = 3 \cdot 11$, so that $\phi(N) = 2 \cdot 10 = 20$.

To find d, we compute $e^{-1} \pmod{20}$ using the extended Euclidean algorithm:

$$\begin{aligned} \boxed{20} &= 1 \cdot \boxed{13} + 7 \\ \boxed{13} &= 2 \cdot \boxed{7} - 1 \end{aligned}$$

Backtracking through this, we find that Bézout's identity takes the form

$$1 = 2 \cdot \boxed{7} - \boxed{13} = 2 \cdot (\boxed{20} - 1 \cdot \boxed{13}) - \boxed{13} = 2 \cdot \boxed{20} - 3 \cdot \boxed{13}.$$

Hence, $13^{-1} \equiv -3 \equiv 17 \pmod{20}$ and, so, $d = 17$.

Comment. Bob's choice of $e=13$ is actually functionally equivalent to $e=3$ (for instance, $5^3 \equiv 26 \pmod{33}$). Similarly, d can be obtained as $e^{-1} \pmod{10}$. Can you explain these claims? □

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

(a) Multiply $x^2 + 1$ and x in $\mathrm{GF}(2^3)$.

(b) Determine the inverse of $x^2 + x$ in $\mathrm{GF}(2^3)$.

Solution.

(a) $(x^2 + 1)x = x^3 + x = 1$ in $\mathrm{GF}(2^3)$.

(b) In general, we use the extended Euclidean algorithm and reduce modulo 2 at each step. Here, we are lucky and are actually done after a single polynomial division:

$$\boxed{x^3 + x + 1} \equiv (x+1) \cdot \boxed{x^2 + x} + 1$$

Hence, $(x^2 + x)^{-1} = x + 1$ in $\mathrm{GF}(2^3)$. □

Problem 5. (16 points) Fill in the blanks.

(a) If Bob's public RSA key is (N, e) and Bob's secret key is d, then how does Bob decrypt the ciphertext c?

The plaintext is $m =$ ______.

(b) For his public RSA key, which of p, q and e must Bob choose randomly? ______

(c) For his public ElGamal key, which of p, g and x must Bob choose randomly? ______

(d) Despite its flaws, in which scenario is it fine to use the Fermat primality test?

______

(e) DES has a block size of ______ bits, a key size of ______ bits and consists of ______ rounds.

(f) To store an S-box in DES as a lookup table, we need ______ bytes.

(g) 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 $c =$ ______. The effective key size is ______ bits.

(h) AES-128 has a block size of ______ bits, a key size of ______ bits and consists of ______ rounds.

(i) The four layers of AES are ______.

(j) For his public ElGamal key, Bob selected $p = 101$. He has ______ choices for g.

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

(l) The primitive roots modulo 5 are ______.

Armin Straub
straub@southalabama.edu

Solution.

(a) The plaintext is $m = c^d \pmod{N}$.

(b) p and q must be chosen randomly.

(c) x must be chosen randomly.

(d) When testing a huge random number for primality.

(e) DES has a block size of 64 bits, a key size of 56 bits and consists of 16 rounds.

(f) Recall that the S-boxes (there is eight different ones) are lookup tables. For each 6 bit input (meaning there is a total of 2^6 possible inputs), they specify 4 bits of output.

To store one S-box, we therefore need to list $2^6 \cdot 4 = 256$ bits, or 32 bytes.

(g) m is encrypted to $c = E_{k_3}(D_{k_2}(E_{k_1}(m)))$.

The effective key size is 112 bits (because of the meet-in-the-middle attack).

(h) AES-128 has a block size of 128 bits, a key size of 128 bits and consists of 10 rounds.

(i) The four layers of AES are: ByteSub, ShiftRow, MixCol, AddRoundKey.

(j) He has $\phi(100) = 40$ choices for g.

(k) Since $\phi(77) = 60$, the smallest choice for e with $e \geqslant 2$ is 7.

(l) The primitive roots modulo 5 are $2, 3$. □

(extra scratch paper)

Armin Straub
straub@southalabama.edu