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.

Solution.

(a) The ciphertext is $c=m^e \pmod{N}$. Here, $c\equiv 7^{13} \pmod{51}$.

$7^2=49\equiv -2$, $7^4\equiv 4$, $7^8\equiv 16 \pmod{51}$. Hence, $7^{13}=7^8\cdot 7^4\cdot 7\equiv 16\cdot 4\cdot 7\equiv 13\cdot 7\equiv 40 \pmod{51}$. Hence, $c=40$.

(b) $N=3\cdot 17$, so that $\phi(N)=2\cdot 16=32$.

To find d, we compute $e^{-1} \pmod{32}$. Either by inspection or using the extended Euclidean algorithm, we find $d=13^{-1}\equiv 5 \pmod{32}$.

Comment. Actually, as discussed in class, $\phi(N)=(p-1)(q-1)=32$ can effectively be replaced with $\operatorname{lcm}(p-1, q-1)=16$. Here, we again get $d=13^{-1}\equiv 5 \pmod{16}$ for the private key.

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?

Solution. If Alice's secret is y and Bob's secret is x, then $10^y\equiv 3$ and $10^x\equiv 12 \pmod{19}$.

We compute $10^2, 10^3, \ldots$ until we find either 3 or 12:

$10^2\equiv 5$, $10^3\equiv 50\equiv 12 \pmod{19}$.

Hence, Bob's secret is $x=3$. The shared secret is $3^3\equiv 8 \pmod{19}$.

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 $\mathrm{GF}(2^4)$.

Solution.

(a) $x^3(x+1) = x^4+x^3 = x^3+x+1$ in $\mathrm{GF}(2^4)$.

(b) We use the extended Euclidean algorithm, and always reduce modulo 2:

$$\begin{aligned}\boxed{x^4+x+1} &\equiv x^2\cdot\boxed{x^2}+(x+1)\\ \boxed{x^2} &\equiv (x+1)\cdot\boxed{x+1}+1\end{aligned}$$

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

$$1 \equiv \boxed{x^2}+(x+1)\cdot\boxed{x+1} \equiv \boxed{x^2}+(x+1)\cdot\left(\boxed{x^4+x+1}+x^2\cdot\boxed{x^2}\right) \equiv (x+1)\boxed{x^4+x+1}+(x^3+x^2+1)\cdot\boxed{x^2}$$

Hence, $(x^2)^{-1} = x^3+x^2+1$ 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 ($\mathrm{IV} = (111)_2$).

Solution. $m = m_1m_2m_3\ldots$ with $m_1 = m_2 = m_3 = 110$.

$c_0 = 111$

$c_1 = E_k(m_1\oplus c_0) = E_k(110\oplus 111) = E_k(001) = 010\oplus 001 = 011$

$c_2 = E_k(m_2\oplus c_1) = E_k(110\oplus 011) = E_k(101) = 110\oplus 001 = 111$

$c_3 = E_k(m_3\oplus c_2) = E_k(110\oplus 111) = E_k(001) = 010\oplus 001 = 011$

Hence, the ciphertext is $c = c_0c_1c_2c_3\ldots = (111\ 011\ 111\ 011\ \ldots)$.

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? [ ]

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

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

$c =$ [ ]. (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

[ ].

(e) DES has a block size of [ ] bits, a key size of [ ] bits and consists of [ ] 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 $c =$ [ ]. The effective key size is [ ] bits.

(g) AES-128 has a block size of [ ] bits, a key size of [ ] bits and consists of [ ] rounds.

(h) Which is the only nonlinear layer of AES? [ ]

(i) For his public ElGamal key, Bob selected $p = 41$. He has [ ] choices for g.

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

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

[ ]

(l) If x has (multiplicative) order 20 modulo 77, then x^8 has order [ ].

Armin Straub
straub@southalabama.edu

(m) The computational Diffie–Hellman problem is: given [ ], determine [ ].

(n) Up to x, there are roughly [ ] many primes.

Solution.

(a) x must be chosen randomly.

(b) p and q must be chosen randomly.

(c) Bob's public ElGamal key is (p, g, h). To send m to Bob, we encrypt it as $c = (g^y, h^y m)$ (all modulo p), where y was randomly chosen.

(d) If the public ElGamal key is (p, g, h), then the private key x can be determined by solving $g^x \equiv h \pmod{p}$.

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

(f) 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).

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

(h) The nonlinear layer of AES is ByteSub.

(i) He has $\phi(\phi(41)) = \phi(40) = \phi(8)\phi(5) = 16$ choices for g.

(j) Since $\phi(77) = \phi(7)\phi(11) = 60$, the smallest choice for e with $e \geqslant 2$ is 7.

(k) 13^x a primitive root modulo 19 if and only if $\gcd(x, 18) = 1$. These x (modulo 18) are $1, 5, 7, 11, 13, 17$. (The total number is $\phi(\phi(19)) = \phi(18) = \phi(2)\phi(9) = 6$.)

(l) If x has (multiplicative) order 20 modulo 77, then x^8 has order $\frac{20}{\gcd(8, 20)} = 5$.

(m) The CDH problem is the following: given $g, g^x, g^y \pmod{p}$, find $g^{xy} \pmod{p}$.

(n) Up to x, there are roughly $x / \ln(x)$ many primes.

Armin Straub
straub@southalabama.edu

(extra scratch paper)

Armin Straub
straub@southalabama.edu