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.

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

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

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 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?

Solution. If Alice's secret is y and Bob's secret is x, then $15^y \equiv 9$ and $15^x \equiv 12 \pmod{19}$.

We compute $15^2, 15^3, \ldots$ until we find either 9 or 12:

$15^2 \equiv (-4)^2 \equiv -3$, $15^3 \equiv -3 \cdot (-4) \equiv 12 \pmod{19}$

Hence, Bob's secret is $x = 3$. The shared secret is $(15^y)^x = 9^3 \equiv 5 \cdot 9 \equiv 7 \pmod{19}$.

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

Solution.

(a) $x^2(x^2+1)=x^4+x^2=x^2+x+1$ 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

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

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

Solution. $m=m_1m_2m_3\ldots$ with $m_1=m_2=m_3=100$.

$c_0=111$

$c_1=E_k(m_1\oplus c_0)=E_k(100\oplus 111)=E_k(011)=101\oplus 110=011$

$c_2=E_k(m_2\oplus c_1)=E_k(100\oplus 011)=E_k(111)=111\oplus 110=001$

$c_3=E_k(m_3\oplus c_2)=E_k(100\oplus 001)=E_k(101)=011\oplus 110=101$

Hence, the ciphertext is $c=c_0c_1c_2c_3\ldots=(111\ 011\ 001\ 101\ \ldots)$.

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

(a) Despite its flaws, it is fine to use the Fermat primality test for [ ].

(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? [ ]

(c) DES has a block size of [ ] bits, a key size of [ ] bits and consists of [ ] rounds.

(d) AES-256 has a block size of [ ] bits, a key size of [ ] bits and consists of [ ] 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 $c =$ [ ]. The effective key size is [ ] bits.

(f) 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.)

(g) For his ElGamal key, which of p, g and x must Bob choose randomly? [ ]

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

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

[ ].

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

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

(l) For his public ElGamal key, Bob selected $p = 53$. He has [ ] choices for g.

Armin Straub
straub@southalabama.edu

(m) 2 is a primitive root modulo 13. For which x is 2^x a primitive root modulo 13? [ ]

(n) If x has (multiplicative) order N modulo m, then x^{10} has order [ ].

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

Solution.

(a) Despite its flaws, it is fine to use the Fermat primality test for large random numbers.

(b) Since $495 \not\equiv \pm 1 \pmod{589}$, we conclude that 589 is not a prime.

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

(d) AES-256 has a block size of 128 bits, a key size of 256 bits and consists of 14 rounds.

(e) 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).

(f) 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.

(g) x must be chosen randomly.

(h) p and q must be chosen randomly.

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

(j) The nonlinear layer of AES is ByteSub.

(k) Since $\phi(65) = 48$, the smallest choice for e with $e \geqslant 2$ is 5.

(l) He has $\phi(\phi(53)) = \phi(52) = \phi(4)\phi(13) = 24$ choices for g.

(m) 2^x a primitive root modulo 13 if and only if $\gcd(x, 12) = 1$. These x (modulo 12) are $1, 5, 7, 11$. (The total number is $\phi(\phi(13)) = \phi(12) = \phi(4)\phi(3) = (4-2)(3-1) = 4$.)

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

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

(extra scratch paper)