550.371/650.471 Cryptology, Final Exam, Spring 2016

Problem 1: (10 points) Factor 145921 using the Quadratic Sieve Method. (Hint: This can be done with only one use of the square root button on your calculator.

Solution:
First, $\sqrt{145921} = 381.99$.
Then note that $382^2 = 3 \bmod 145921$ and also $383^2 = 768 = 2^8 \cdot 3 \bmod 145921$.
Thus $(382 \cdot 383)^2 = (2^4 \cdot 3)^2 \bmod 145921$
that is, $385^2 = 48^2 \bmod 145921$
So $\gcd(385 - 48, 145921) = 337$ or, alternatively, $\gcd(385 + 48, 145921) = 433$

Problem 2: (10 points) Suppose that n is an odd, composite integer; in particular, say that $n = a \cdot b$, where $a \leq b$ are nontrivial factors (and a, b are obviously odd). Prove that Fermat Factorization will eventually factor n. Use your answer to briefly explain a takeaway lesson for RSA.

Solution: When $i = \frac{b-a}{2}$ (which is an integer because a, b are odd, hence $b - a$ is even) then $n + i^2 = ab + (\frac{b-a}{2})^2 = ab + \frac{b^2-2ab+a^2}{4} = \frac{b^2+2ab+a^2}{4} = (\frac{b+a}{2})^2$, and $\frac{b+a}{2}$ is an integer since $b + a$ is even. Thus, $n = (\frac{b+a}{2})^2 - (\frac{b-a}{2})^2 = (\frac{b+a}{2} - \frac{b-a}{2}))(\frac{b+a}{2} + \frac{b-a}{2}) = a \cdot b$.
The takeaway lesson is not to choose RSA modulus using primes that are near each other.

Problem 3: (10 points) Compute $5^{24} \mod 11$ **specifically** using fast exponentiation.

Solution: We first express $24 = 2^3 + 2^4$. Then we successively square to get
$5^{2^0} = 5 \mod 11$
$5^{2^1} = 5^2 = 25 = 3 \mod 11$
$5^{2^2} = 3^2 = 9 \mod 11$
$5^{2^3} = 9^2 = 81 = 4 \mod 11$
$5^{2^4} = 4^2 = 16 = 5 \mod 11$
Thus we have $5^{24} = 5^{2^4} \cdot 5^{2^3} = 5 \cdot 4 = 9 \mod 11$.

Problem 4: (10 points) The integer 10573 is a product of the primes 97 and 109. Find the value x such that $0 \leq x < 10573$, and x simultaneously solves the equations:
$x \equiv 48 \bmod 97$ and also
$x \equiv 27 \bmod 109$.
Hint: It may be useful to use the fact that $9 \cdot 97 - 8 \cdot 109 = 1$.

Solution: $x \equiv 48 \cdot 109 \cdot (-8) + 27 \cdot 97 \cdot 9 = -18285 = 2861 \bmod 10573$.

Problem 5: (10 points) Alice and Bob did a Diffie-Hellman Key Exchange; this consisted of first agreeing on the prime number 11 and the primitive root 8 mod 11. Then Alice sent Bob 10 mod 11 as "A", and Bob sent Alice 6 mod 11 as "B". Suppose that you intercept these A and B. Compute the particular key k which was exchanged here. Hint: Because p is small, you are able to compute discrete logarithms.

Solution: The powers of 8 mod 11, ie $8^0, 8^1, 8^2, \ldots$ are, respectively, $1, 8, 9, 6, 4, 10, 3, 2, 5, 7$. Thus $a = \text{dlog}_8 10 = 5$ mod 11 and, alternatively, $b = \text{dlog}_8 6 = 3$ mod 11. Thus the key is $k = A^b = 10^3 = 10$ mod 11 and, alternatively, $k = B^a = 6^5 = 10$ mod 11.

Problem 6: (10 points) Suppose Alice and Bob have the same RSA modulus n, and suppose their encryption exponents e_A and e_B happen to be relatively prime. Charles wants to send the same message $m \in \mathbb{Z}_n^*$ to both Alice and Bob, so he encrypts $c_A = m^{e_A}$ mod n and $c_B = m^{e_B}$ mod n. Prove how Eve can efficiently compute m if she intercepts c_A and c_B.

Solution: Since $\gcd(e_A, e_B) = 1$, Eve can compute (efficiently with Extended Euclid Algorithm) $x, y \in \mathbb{Z}$ such that $x \cdot e_A + y \cdot e_B = 1$. Then Eve can compute (efficiently with fast exponentiation) $c_A^x c_B^y = (m^{e_A})^x (m^{e_B})^y = m^{x \cdot e_A + y \cdot e_B} = m^1 = m$ mod n.

Problem 7: (10 points) What two things (facts, abilities,...) do we need in order for us to be sure that we can efficiently generate large prime numbers? You may not mention any names of mathematicians, dead or otherwise.

Solution: We need to know that the prime numbers are dense enough; indeed, the Prime Number Theorem provides us with this. We also need an efficient algorithm for testing primality. With these two things we are equipped to randomly pick numbers and test for primality and be successful in a reasonable amount of time.

Problem 8: (10 points) Recall that when we were analyzing the Quadratic Sieve method for factoring n, we made a particular matrix whose columns represented numbers whose squares were close to multiples of n, and whose rows represented "small primes." Remind me of a condition on this matrix that would guarantee the existence of the desired perfect squares of small primes. Short answer!

Solution: More columns than rows.

Problem 9: (10 points) **a)** State and prove a theorem that gives us an upper bound on the number of iterations of Euclid Algorithm, from which we have that Euclid Algorithm is efficient.
b) Explain how the upper bound from part **a)** results in efficiency of Euclid Algorithm. (You need to say what it means for an algorithm to be efficient, and demonstrate that Euclid fits the bill.)

Problem 10: (10 points). Suppose that n is a composite, odd number that we want to test for primality, and we will use the base a.
a) Show that if Miller-Rabin Test is fooled then Fermat Test is fooled.
b) Suppose Fermat Test is fooled– and Miller Rabin Test is not. Explain a fringe benefit, and be clear exactly what mechanism you will use to get this fringe benefit.

SCRAP PAPER This page will not be graded.

SCRAP PAPER This page will not be graded.