CS 4801: Assignment 3

Adam Camilli (aocamilli@wpi.edu)

Wednesday 28$^{\text{th}}$ November, 2018

1. **Computing RSA by hand.** Let $p = 43; q = 37; b = 23$ be your initial parameters. You may use a calculator for this problem, but you should show all intermediate results.

   (a) **Key generation**: Compute N and $\phi(N)$. Compute the private key

   $$k_{\text{priv}} = a = b^{-1} \bmod \phi(N)$$

   using the extended Euclidean algorithm. Show all intermediate results.

   1. Choose two prime numbers p, q:

      $$p = 43, q = 37 \qquad \text{(given)}$$

   2. Compute N:

      $$N = p \cdot q = 43 \cdot 37 = 1591$$

   3. Compute $\phi(N)$:

      $$\phi(N) = (p-1)(q-1) = 42 \cdot 36 = 1512$$

   4. Choose random $b \mid 0 < b < \phi(N)$ with $\texttt{gcd}(b, \phi(N)) = 1$:

      $$b = 23 \qquad \text{(given)}$$

   5. Compute a:

      $$a = b^{-1} \bmod \phi(N) = 23^{-1} \bmod 1512$$

      (Next Page)

$$
\begin{array}{lll}
s_0: & 1512 = \mathbf{65}(23) + 17 & p_0 = 0 \text{ (given)} \\
s_1: & 23 = \mathbf{1}(17) + 6 & p_1 = 1 \text{ (given)} \\
s_2: & 17 = \mathbf{2}(6) + 5 & p_2 = p_0 - p_1(q_0) \bmod 1512 \\
 & & \quad = 0 - 1(65) \bmod 1512 = 1447 \\
s_3: & 6 = \mathbf{1}(5) + 1 & p_3 = p_1 - p_2(q_1) \bmod 1512 \\
 & & \quad = 1 - 1447(1) \bmod 1512 = 66 \\
s_4: & 5 = \mathbf{1}(5) + 0 & p_4 = p_2 - p_3(q_2) \bmod 1512 \\
 & & \quad = 1447 - 66(2) \bmod 1512 = 1315 \\
 & & p_5 = p_3 - p_4(q_3) \bmod 1512 \\
 & & \quad = 66 - 1315(1) \bmod 1512 = \mathbf{263}
\end{array}
$$

$$k_{\text{priv}} = 263$$

(b) **Encryption**: Encrypt the message $X = 91$ by applying the square and multiply algorithm (first, transform the exponent to binary representation). Show all intermediate results.

The encrypted message is calculated

$$\begin{aligned} Y = \texttt{Enc}(X) &= X^b \bmod N \\ &= 91^{23} \bmod 1591 \end{aligned}$$

Convert exponent b to binary:

$$23_{10} = 2^4 + 2^3 - 1 = 11000_2 - 1 = 10111_2$$

Now execute square and multiply for $91^{23} \bmod 1591$:

b	Algorithm step	mod reduction
1	91	$91 \bmod 1591 = \mathbf{91}$
0	$(91)^2$	$(91)^2 \bmod 1591 = \mathbf{326}$
1	$((91)^2)^2 \cdot 91$	$(326)^2 \cdot 91 \bmod 1591 = \mathbf{1018}$
1	$(((91)^2)^2 \cdot 91)^2 \cdot 91$	$(1018)^2 \cdot 91 \bmod 1591 = \mathbf{550}$
1	$((((91)^2)^2 \cdot 91)^2 \cdot 91)^2 \cdot 91$	$(550)^2 \cdot 91 \bmod 1591 = \mathbf{18}$

$$\texttt{Enc}(X) = 18$$

(c) **Decryption**: Decrypt the ciphertext Y computed above by applying the square and multiply algorithm. Show all intermediate results.

The decrypted message is calculated

$$\begin{aligned} X = \texttt{Dec}(Y) &= X^{k_{priv}} \bmod N \\ &= 18^{263} \bmod 1591 \end{aligned}$$

Convert exponent b to binary:

$$263_{10} = 2^8 + 2^3 - 1 = 100000000_2 + 1000_2 - 1 = 100000111_2$$

Now execute square and multiply for $18^{263} \bmod 1591$:

b	Algorithm step	mod reduction
1	18	$18 \bmod 1591 = \mathbf{18}$
0	$(18)^2$	$(18)^2 \bmod 1591 = \mathbf{324}$
0	$((18)^2)^2$	$(324)^2 \bmod 1591 = \mathbf{1561}$
0	$(((18)^2)^2)^2$	$(1561)^2 \bmod 1591 = \mathbf{900}$
0	$((((18)^2)^2)^2)^2$	$(900)^2 \bmod 1591 = \mathbf{181}$
0	$(((((18)^2)^2)^2)^2)^2$	$(181)^2 \bmod 1591 = \mathbf{941}$
1	$((18)^{16})^2 \cdot 18$	$(941)^2 \cdot 18 \bmod 1591 = \mathbf{20}$
1	$((18)^{32})^2 \cdot 18$	$(20)^2 \cdot 18 \bmod 1591 = \mathbf{836}$
1	$((18)^{64})^2 \cdot 18$	$(836)^2 \cdot 18 \bmod 1591 = \mathbf{91}$

$$\texttt{Dec}(Y) = X = 91$$

2. Eve records the transmission of an RSA-encrypted message in Question 1. Eve also knows the public key to be $k_{pub} = (N, b)$. Your goal is to recover the message X that has been encrypted with RSA in Question 1 Part b.

   (a) Give the equation for the decryption of Y. Which variables are not known to Eve? Can Eve recover X? If so, how? If not, why?

   $$\texttt{Dec}(Y) = Y^{k_{priv}} \bmod N$$

   In this equation, the encrypted message Y is given to Eve, and N is available as part of k_{pub}. k_{priv} is unknown to Eve. Eve cannot easily decrypt Y without deriving k_{priv} however, since she cannot perform the calculation.

   (b) To recover the private key a, Eve has to compute $a = b - 1 \bmod \phi(N)$. Can Eve recover $\phi(N)$?

   Yes. Eve knows that in RSA k_{priv} is generated using N, which is a product of two primes p and q. k_{priv} is calculated using the value $\phi(N)$ which is equivalent to $(p - 1)(q - 1)$. In order to find this value she must factorize N. The computational difficulty of factoring large N is the foundation of RSA's security, since if this is done the rest of the calculation of k_{priv} is comparatively trivial.

(c) Compute the message X. (Hint: Start by factoring $N = p \cdot q$. Then use $\phi(N)$ to compute b)

$$\sqrt{|N|} \approx 39.89$$

Therefore it is sufficient to check N's divisibility with primes less than or equal to 39:

$$\text{primes } = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$$

$\frac{1591}{2}$	$\varnothing$
$\frac{1591}{3}$	$\varnothing$
$\frac{1591}{5}$	$\varnothing$
$\frac{1591}{7}$	$\varnothing$
$\frac{1591}{11}$	$\varnothing$
$\frac{1591}{13}$	$\varnothing$
$\frac{1591}{17}$	$\varnothing$
$\frac{1591}{23}$	$\varnothing$
$\frac{1591}{29}$	$\varnothing$
$\frac{1591}{31}$	$\varnothing$
$\frac{1591}{33}$	$\varnothing$
$\frac{1591}{37}$	43

We now know $N = p \cdot q = 37 \cdot 43$. $\phi(N)$ is therefore $(p-1)(q-1) = 36 \cdot 42 = 1512$.
Since we are given public key exponent $b = 23$, we can now calculate a and decrypt Y as in problem 1:

$$a = 23^{-1} \bmod 1512 = 263$$

$$\texttt{Dec}(Y = 18) = X = 91$$

(d) Can Eve do the same message recovery attack (as in (c)) for large N, e.g., $|N| = 1024$ bit?

Technically yes, however presently (2018) the factorization of N would take several millenia to accomplish using the fastest algorithm (general number field sieve) on supercomputers. Eve therefore would likely not be able to use this attack.

(e) Eve recovers a message-ciphertext pair (X, Y). Can she recover the private key a?

Even if no random padding is performed (as would be recommended in real life) Eve can still not feasibly compute a with (X, Y). Were this case, RSA would not be a correct public-key encryption algorithm, since any user can calculate an arbitrary (X, Y) using a public key. Detecting a this way would be equivalent to guessing, since Eve's only option is to try and reproduce Y by encrypting X using different possible values of a.

3. Find the following using Extended Euclidean Algorithm

   (a) Find $17^{-1} \bmod 37$ using Extended Euclidean Algorithm

During each step s_i, recursively calculate

$$p_i = p_{i-2} - p_{i-1}q_{i-2} \bmod n$$

q_i is equal to the coefficient on the left side (bolded). Repeat until remainder is 0 and iterate right side (p calcuation) one more time.

$$\texttt{gcd}(17, 37) = 1$$

$$\therefore \exists \text{ integers } (p, n) \mid 17p = 37n + 1$$

$$\begin{aligned}
&s_0: \ 37 = \mathbf{2}(17) + 3 && p_0 = 0 \text{ (given)} \\
&s_1: \ 17 = \mathbf{5}(3) + 2 && p_1 = 1 \text{ (given)} \\
&s_2: \ 3 = \mathbf{1}(2) + 1 && p_2 = p_0 - p_1(q_0) \bmod 37 \\
& && \quad = 0 - 1(2) \bmod 37 = 35 \\
&s_3: \ 2 = \mathbf{2}(1) + 0 && p_3 = p_1 - p_2(q_1) \bmod 37 \\
& && \quad = 1 - 35(5) \bmod 37 = 11 \\
& && p_4 = p_2 - p_3(q_2) \bmod 37 \\
& && \quad = 35 - 11(1) \bmod 37 = \mathbf{24}
\end{aligned}$$

Modular inverse is **24**

   (b) Find $13^{-1} \bmod 91$

$$\texttt{gcd}(13, 91) = 13$$

$$\therefore \nexists \text{ integers } (p, n) \mid 13p = 91n + 1$$

13 not invertible modulo 91

(c) Find $13^{-1} \bmod 448$

$$\texttt{gcd}(13, 448) = 1$$

$$\therefore \exists \text{ integers } (p, n) \mid 13p = 448n + 1$$

$$\begin{array}{ll}
s_0: \; 448 = \mathbf{34}(13) + 4 & p_0 = 0 \text{ (given)} \\
s_1: \; 13 = \mathbf{2}(6) + 1 & p_1 = 1 \text{ (given)} \\
s_2: \; 6 = \mathbf{6}(1) + 0 & p_2 = p_0 - p_1(q_0) \bmod 448 \\
 & \quad = 0 - 1(34) \bmod 448 = 414 \\
 & p_3 = p_1 - p_2(q_1) \bmod 448 \\
 & \quad = 1 - 414(2) \bmod 448 = \mathbf{69}
\end{array}$$

Modular inverse is **69**

(d) Find $16^{-1} \bmod 4725$

$$\texttt{gcd}(16, 4725) = 1$$

$$\therefore \exists \text{ integers } (p, n) \mid 16p = 4725n + 1$$

$$\begin{array}{ll}
s_0: \; 4725 = \mathbf{295}(16) + 5 & p_0 = 0 \text{ (given)} \\
s_1: \; 16 = \mathbf{3}(5) + 1 & p_1 = 1 \text{ (given)} \\
s_2: \; 5 = \mathbf{5}(1) + 0 & p_2 = p_0 - p_1(q_0) \bmod 4725 \\
 & \quad = 0 - 1(295) \bmod 4725 = 4430 \\
 & p_3 = p_1 - p_2(q_1) \bmod 4725 \\
 & \quad = 1 - 4430(3) \bmod 4725 = \mathbf{886}
\end{array}$$

Modular inverse is **886**