Information Systemls Security .
Series 5 Correction

November 17th, 2021

Exercise 1 : RSA

- $n = p \cdot q = 11 \cdot 17 = 187$, $\Phi(n) = 160$.
  Let's choose e prime with $\Phi(n)$, for example e = 7. Then we have to find the corresponding decryption exponent d = 23 ($7 \cdot 23 \equiv 161 \equiv 1 \mod 160$).
  We have public key (187,7) and private key (187,23).

- $28^{41} \mod 247$.
  $28^2 \equiv 43 \mod 247$
  $28^4 \equiv 120 \mod 247$
  $28^8 \equiv 74 \mod 247$
  $28^{16} \equiv 42 \mod 247$
  $28^{32} \equiv 35 \mod 247$
  Then we can compute $28^{41} \equiv 28^{32} \cdot 28^8 \cdot 28 \equiv 35 \cdot 74 \cdot 28 \equiv 149 \mod 247$.
  So the ciphertext is c = 149.

- First, we need to factorize $n = 247 = 13 \cdot 19$. Then, we compute $\Phi(n) = (p-1)(q-1) = 216$. And now we can compute the decryption exponent d corresponding to our encryption exponent e=41 :

  We find d=137. To find it, we're using Euclide's extended algorithm :

  We have $a = \Phi(n) = 216$ and $b = e = 41$. So we're starting with :

  $r_0 = a = 216$
  $r_1 = b = 41$
  $s_0 = 1$
  $s_1 = 0$
  $t_0 = 0$
  $t_1 = 1$
  $q_1 = r_0 \div r_1 = 5$

Then we have :

$r_2 = r_0 - q_1 \cdot r_1 = 216 - 5 \cdot 41 = 11$
$s_2 = s_0 - q_1 \cdot s_1 = 1 - 5 \cdot 0 = 1$
$t_2 = t_0 - q_1 \cdot t_1 = 0 - 5 \cdot 1 = -5$
$q_2 = r_1 \div r_2 = 41 \div 11 = 3$

$r_3 = r_1 - q_2 \cdot r_2 = 41 - 3 \cdot 11 = 8$
$s_3 = s_1 - q_2 \cdot s_2 = 0 - 3 \cdot 1 = -3$
$t_3 = t_1 - q_2 \cdot t_2 = 1 - 3 \cdot -5 = 16$
$q_3 = r_2 \div r_3 = 11 \div 8 = 1$

Similarly, we find :

$r_4 = 3$
$s_4 = 4$
$t_4 = -21$
$q_4 = 2$

$r_5 = 2$
$s_5 = -11$
$t_5 = 58$
$q_5 = 1$

$r_6 = 1$
$s_6 = 15$
$t_6 = -79$
$q_6 = 2$

And finally, we have $r_7 = 0$. So $r_{i+1} = r_7 = 0$, and the desired results are r_6, s_6 et t_6 :

- $pgcd(\Phi(n), e) = r_6 = 1$ (that's expected, as e is chosen such that $\Phi(n)$ and e are co-prime,
- s_6 is the inverse of $\Phi(n)$ modulo e (not used here),
- And finally, what we want, $t_6 = -79$, which is almost the inverse of e modulo $\Phi(n)$ (it's not in $\mathbb{Z}_{\Phi(n)}$, as Bézout sometimes gives negative coefficients, so we just have to apply a modulo $\Phi(n)$ to find the decryption exponent d :

  $d = t_6 \mod \Phi(n) = -79 \mod 216 = 137.$

  The decryption exponent is d=137 (And we can see that $41 \cdot 137 \equiv 5617 \equiv 26 \cdot 216 + 1 \equiv 1 \mod 216$).

Finally, let's verify by deciphering the previous cipher : $m = 149^{137} \mod 247$

$149^2 \equiv 218 \mod 247$
$149^4 \equiv 100 \mod 247$

$149^8 \equiv 120 \mod 247$
$149^{16} \equiv 74 \mod 247$
$149^{32} \equiv 42 \mod 247$
$149^{64} \equiv 35 \mod 247$
$149^{128} \equiv 237 \mod 247$

And we have $149^{137} \equiv 149^{128} \cdot 149^8 \cdot 149 \equiv 237 \cdot 120 \cdot 149 \equiv 28 \mod 247$
We find the initial message "28" as expected.

Exercise 2 : Rabin

- $134^2 \equiv 17956 \equiv 246 \mod 253$. The ciphertext send is c = 246.
- We're factorizing $n = 253 = 11 \cdot 23$. We have p=11 and q=23.
- Then we compute m_p, m_q, p_1 and q_1 :

$$m_p = 246^3 \mod 11 \equiv 4^3 \mod 11 = 9$$
$$m_q = 246^6 \mod 23 \equiv 16^6 \mod 11 \equiv 3^3 \mod 11 = 4$$
$$p_1 = p^{-1} \mod q = 11^{-1} \mod 23 = 21$$
$$q_1 = q^{-1} \mod p = 23^{-1} \mod 11 = 1$$

And finally the 4 possible messages :

$$m_1 = (m_p \cdot q \cdot q_1 + m_q \cdot p \cdot p_1) \mod n = 207+924 \mod 253 \equiv 1131 \mod 253 = 119$$
$$m_2 = 207 - 924 \mod 253 \equiv -717 \mod 253 = 42$$
$$m_3 = -207 + 924 \mod 253 \equiv 717 \mod 253 = 211$$
$$m_4 = -207 - 924 \mod 253 \equiv -1131 \mod 253 = 134$$

And we can see that m_4 was our original message.

Exercise 3 : ElGamal

- Let's choose a random k, for example k=7, we have $\lambda = \alpha^k \mod p = 3^7 \mod 17 = 11$ and $\sigma = m \cdot (\alpha^a)^k \mod p = 2 \cdot 12^7 \mod 17 \equiv 2 \cdot 7 \mod 17 = 14$. Then we send $(\lambda,\sigma) = (11,14)$.
- We compute all powers of $\alpha = 3$ modulo $p = 17$, and find that $3^{13} \equiv 12 \mod 17$, so the private key is $a = 13$.
- First we compute $x = \lambda^{p-1-a} \mod p = 11^3 \mod 17 = 5$. Then $m = x \cdot \sigma \mod p = 5 \cdot 14 \mod 17 \equiv 70 \mod 17 = 2$.
  And that's effectively our initial message.

Exercise 4 : Conclusion

- These are not unbreakable, because we just found all Alice's private keys by force.
- That's because the reliability of these algorithms is based on having big numbers, that makes them very hard to compute by force. These need numbers of at the very least 1024 bits (and that's a minimum, nowadays we're taking more to ensure they're not breakable). We were able to find Alice keys because the numbers were really small. Still, these algorithms may suffer in the future, slowly because of the increasing computing power at our disposal, and they may even be doomed by the rising of quantum computers.