International program of Isima
Academic year 2015-2016

Network security (second session)

Allowed: handwritten documents, printed course notes from the website, paper dictionaries.
Forbidden: books, mobile phones, calculators, electronic translators.
Duration: 2 hours

1. Differential cryptanalysis of DES (5 points)

Figure 1 shows the S-box 5 of DES. It can be seen that $S_5(110110)=5_{10}$ (because line is *1----0* and column is *-1011-*).

S_5	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
01	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
10	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Figure 1: The S-box 5 of DES.

Question 1.1 (0.5 point): What is the value of $S_5(110111)$ in decimal?
Question 1.2 (0.5 point): How many possible inputs are there for S_5?
Question 1.3 (4 points): Let us write $O_1=S_5(I_1)$ and $O_2=S_5(I_2)$. Let us assume that $I_1 \oplus I_2=100000$ (where $\oplus$ denotes the XOR operation), and that $O_1 \oplus O_2=1110$. We assume that I_1 is between 0 and 15_{10} (in order to reduce the amount of values to verify). What are the possible values for I_1 (out of these 16 values)?

2. Elliptic curve cryptography (5 points)

Let us consider the elliptic curve $E=\{(x,y)|y^2=x^3+x+6 \bmod 11\}$.
Question 2.1 (1 point) : Fill the following table.

y	0	1	2	3	4	5	6	7	8	9	10
$y^2 \bmod 11$											

Question 2.2 (1 point) : What are the possible values for y, when $y^2=3$? What are the possible values for y, when $y^2=8$?
Question 2.3 (1 point) : Compute the thirteen points of E, with $0 \leq x<11$. Do not forget the point $O=(+\infty,+\infty)$. Note that $5^3 \bmod 11=4$, $6^3 \bmod 11=7$, $7^3 \bmod 11=2$, $8^3 \bmod 11=6$, $9^3 \bmod 11=3$, and $10^3 \bmod 11=10$.

For the next two questions, you can base your intuition on the geometrical approach for the elliptic curve $\{(x,y)| y^2=x^3+x+6\}$ (although E does not contain all the points).
Question 2.4 (1 point): What is the value of $(2,7)+(2,4)$?
Question 2.5 (1 point): What is the value of $(3,5)+O$?

3. Factorization attacks on RSA (10 points)

Most attacks on the cryptographic algorithm RSA are based on the factorization of n from the public key (e,n).
Question 3.1 (0.5 point): Explain why the factorization of n can be used to cryptanalyze RSA.
Question 3.2 (0.5 point): Why is it important to use large factors for n?

A simple factorization attack is based on identifying a small number b such that $a^2-b^2=n$, with $a=ceil(sqrt(n))$.

Question 3.3 (0.5 point): Show that in this case, $n=(a-b)(a+b)$.

Question 3.4 (1 point): Given the fact that $ceil(sqrt(4891))=70$, find a factorization of 4891.

Question 3.5 (0.5 point): Why does this method work only when both factors of n are close to the square root of n?

Some sophisticated attacks have been developed for small d. They are based on the identification of weak values of e that make the factorization of n simple.

Question 3.6 (1 point): If $e=k.q$, with $1<k<p$, then $n=p.q$ can be factorized easily.

- Prove this property.
- How many values of e are weak, using this property?

Question 3.7 (1 point): Wiener [2] showed that from any public exponent e that corresponds to a secret exponent d with $d\leq(1/3)n^{1/4}$, n can be factorized in time polynomial in $log(n)$.

- If n has a size of 1024 bits, how many values of e are weak, using this property?
- Does this make a large amount of weak keys?

Question 3.8 (1 point): Howgrave-Graham [3] showed that the knowledge of $e=kq+r$, with $r\leq n^{1/4}$, allows to find the factorization of n. How many values of e are weak in this case? You can assume that both factors of n are close to $sqrt(n)$.

Blömer and May attack [1] states that if $e.x+y=k.phi(n)$, with k an integer, $0<x\leq(1/3)n^{1/4}$ and $|y|=O(n^{-3/4}.e.x)$, then n can be factorized. They use the fact that the keys in this case are such that $e^{-1}=d=-x/y\ [phi(n)]$.

Question 3.9 (1.5 point): Show that this attack generalizes the Wiener's attack for a given value of x and of y.

Question 3.10 (1 point): Show that x and y are small.

Question 3.11 (1.5 points): Note that d and e are not necessarily small. Explain why it might be difficult for an user to identify such values of e as weak keys.

4. References

[1] J. Blömer, A. May. “A generalized Wiener attack on RSA”, in Proceedings of Public Key Cryptography, 2004.

[2] M. Wiener. “Cryptanalysis of short RSA secret exponents”, IEEE Transactions on Information Theory, vol. 36, pp. 553—558, 1998.

[3] N. Howgrave-Graham. “Approximate integer common divisors”, Cryptography and Lattices, Lecture Notes in Computer Science, vol. 2146, Springer-Verlag, 2001.