Univ. Grenoble Alpes/Grenoble INP **2016–2017**

M2 Cybersecurity

Exercises and problems for Crypto's lectures

Questions on symmetric ciphers

1 We consider the alphabet $\mathscr{A} = \{1,2,3,4,5,6\}$ and the mathematical substitution

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 1 & 5 \end{pmatrix}.$$

Encrypt by *substitution* (in the cryptographic meaning) the plaintext 216452.
Encrypt by *permutation* (in the cryptographic meaning) the plaintext 216452.

2 We consider the alphabet $\mathscr{A} = \{1,2,3,4,5,6\}$ and the mathematical substitution

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 5 & 1 & 3 \end{pmatrix}.$$

Encrypt by *substitution* (in the cryptographic meaning) the plaintext 216351.
Encrypt by *permutation* (in the cryptographic meaning) the plaintext 216351.

3 Prove that the decryption in a Feistel cipher can be done by applying the encryption algorithm to the ciphertext, with the key schedule reversed (and entries swaped as given in the lectures).

4 Let $DES(x,K)$ be the DES encryption of the plaintext x with the key K. Denote, for any binary quantity X, by $\bar{X}$ the bitwise complement of X. Consider $y = DES(x,K)$ and $y' = DES(\bar{x},\bar{K})$. Show that $y' = \bar{y}$ (i.e., the ciphertext is also complemented).

5 *A basic differential cryptanalysis on* S_1 *:* Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function representing an "abstract" S-box. F or any $\delta_I \in \mathbb{F}_2^n$ and $\delta_O \in \mathbb{F}_2^m$, we define

$$\Delta'_F(\delta_I,\delta_O) = \{(x_1,x_2;y_1,y_2),\ y_1 = F(x_1),\ y_2 = F(x_2),\ x_1,x_2 \in \mathbb{F}_2^n,\ y_1,y_2 \in \mathbb{F}_2^m,\ x_1 \oplus x_2 = \delta_I,\ y_1 \oplus y_2 = \delta_O\}.$$

We call δ_I and δ_O respectively the input and output XOR differences.

(a) Compute $\Delta'_F(0,\delta)$ for any $\delta \in \mathbb{F}_2^m$ with $\delta \neq 0$. Compute the cardinality of $\Delta'_F(0,0)$.

(b) Show that for any $\delta_I \in \mathbb{F}_2^n$ and $\delta_O \in \mathbb{F}_2^m$, the cardinality of the set $\Delta'_F(\delta_I,\delta_O)$ is even (remember that 0 is an even number).

(c) Express $\Delta'_F(\delta_I,\delta_O)$ as a set $\Delta_F(a,b)$ (as seen in the lectures), with adequates a and b depending of δ_I and δ_O (i.e., for a and b well choosen, we have $\Delta'_F(\delta_I,\delta_O)$ in bijection with $\Delta_F(a,b)$).

(d) Show that each entry (x,y) of a differential distribution table of a DES S-box F, corresponds to the cardinality of $\Delta'_F(x,y)$. *We will denote by* $\Delta'_i(x,y)$ *the set* $\Delta'_F(x,y)$ *with* $F = S_i$ *the ith S-box of the DES.*

(e) Compute $\Delta'_1(60,2)$ (values are in decimal).

(f) We consider the 6-bit partial key k of a DES S-box F. Assume that the values x_1,x_2 (hence $x_1 \oplus x_2 = \delta_I$) and δ_O are known (with respect to F). Show that $x_i \oplus k \in \Delta'_F(\delta_I,\delta_O)$ for $i = 1,2$. Deduce a method for recovering the partial key k.

(g) Set $F = S_1$. We give the following table of values (in decimal)

x_1	x_2	δ_O
33	56	1
20	35	2
20	28	9

Recover the corresponding 6-bit partial key k of S_1.

6 *Unusual properties of the DES box S_4 :*

(a) Prove that the second row of S_4 can be obtained from the first row by means of the following mapping :

$$(y_1, y_2, y_3, y_4) \mapsto (y_2, y_1, y_4, y_3) \oplus (0,1,1,0),$$

where the entries are represented as binary strings.

(b) Show that any row of S_4 can be transformed into any other row by a similar type of operation.

Questions on AES

Questions on Finite Fields (related to AES)

1 How can you check the irreducibility of a polynomial of degree less than 3 over a finite field? What can you do for higher degrees?

2 Find all the irreducible polynomials of degree less than 5 over $\mathbb{F}_2$.

3 Construct $\mathbb{F}_4$ using an irreducible polynomial of degree 2 over $\mathbb{F}_2$. Give explicitly its multiplication table.

4 Find all the irreducible polynomials of degree 2 over $\mathbb{F}_4$.

5 Construct $\mathbb{F}_{16}$ using an irreducible polynomial of degree 2 over $\mathbb{F}_4$. Give explicitly its multiplication table.

6 Construct $\mathbb{F}_{16}$ using an irreducible polynomial of degree 4 over $\mathbb{F}_2$. Compare with the results of the previous question.

7 Construct $\mathbb{F}_{256}$ as extension of degree 8 over $\mathbb{F}_2$, as extension of degree 4 over $\mathbb{F}_4$ and as extension of degree 2 over $\mathbb{F}_{16}$. Using PARI/GP, compare the different table of multiplications. Give explicit isomorphisms between the three constructions.

Inversion in $\mathbb{F}_{256}$ and the AES S-box

In the following we will use the AES representation of $\mathbb{F}_{256}$ (using the specific irreducible polynomial of degree 8 over $\mathbb{F}_2$). The inversion table in $\mathbb{F}_{256}$ is given by the following table :

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	**0**	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2
2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2
3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19
4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09
5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17
6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b
7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82
8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4
9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a
a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62
b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57
c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6
d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b
e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	e3	5d	50	1e	b3
f	5b	23	38	34	68	46	03	8c	dd	9c	7d	a0	cd	1a	41	1c

Recall that an element of $\mathbb{F}_{256}$ can be represented in hexadecimal notation as $(XY)_{hex}$ with X and Y two hexadecimal numbers. *The **0** value is an AES convention and has no mathematical meaning.* In order to compute its inverse, X will denote the row number and Y the column number in the above table. Then the inverse of $(XY)_{hex}$ is given by the corresponding entry in the table.

For instance, using the notation seen in the lectures, if $x^7 + x^6 + x$ is an element of $\mathbb{F}_{256}$, then as binary we have $(11000010)_2$. This corresponds in hexadecimal representation to $(c2)_{hex}$. Thus, its inverse is given by the entry corresponding to the row c and the column 2, namely $(2f)_{hex} = (00101111)_2 = x^5 + x^3 + x^2 + x + 1$.

Recall that the AES S-box is given by the following table (using the same notation as above) :

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	b	db
a	e0	32	3a	a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	3	f6	e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	d	bf	e6	42	68	41	99	2d	f	b0	54	bb	16

For instance, if we want to compute $S_{AES}((c2)_{hex})$, we look at the entry corresponding to the row c and the column 2. The result is $(25)_{hex}$. But according to the SAC lectures, the S-box is also described as the following linear map φ_{AES} over $\mathbb{F}_2$:

$$\varphi_{AES}(X) = \begin{pmatrix} Z_0 \\ Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \\ Z_5 \\ Z_6 \\ Z_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \\ Y_5 \\ Y_6 \\ Y_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

with $Z = (Z_7 Z_6 \cdots Z_0)$. We have $S_{AES}(X) = \varphi_{AES}(X^{-1})$ (or equivalently $S_{AES}(X) = \varphi_{AES}(Y)$ with Y the inverse of X). If $X = (11000010)_2 = (c2)_{hex}$, then its inverse is $Y = (2f)_{hex} = (00101111)_2$. Applying the above map, we get $Z = (00100101)_2 = (25)_{hex}$.

1 Check that the inverse of $x^7 + x^6 + x$ is $x^5 + x^3 + x^2 + x + 1$ (as computed according to the table).

2 Compute the inverse of $x + x^2$ and $1 + x + x^7$. Check the results.

3 Check that the image of $(11000010)_2$ by the linear map φ_{AES} is indeed $(00100101)_2$

4 Compute $S_{AES}(x + x^2)$ and $S_{AES}(1 + x + x^7)$ using the S-box table, and checking the results using the inversion table and the linear map.

5 Using PARI/GP, check that the $S_{AES}(X) = \varphi_{AES}(X^{-1})$ for all $X \in \mathbb{F}_{256}$.

6 Compute (using PARI/GP) the inverse of φ_{AES}. Deduce the inverse of S_{AES}.

Questions on RSA and asymmetric ciphers

1 (A general question unrelated to RSA) In order to create our passwords we use an alphabet made of 128 (distinct) characters. We need to design a passphrase for protecting our electronic wallet containing several private keys. We suppose that the ciphers associated to our private keys are theoretically breakable in 2^{512} operations. In order to be consistant with our choices of cryptosystems, how long our passphrase should be?

2 Can we turn an asymmetric cipher into a symmetric cipher? (justify your answer by either proposing a symmetric scheme from an asymmetric cipher or by proving that it is not possible)

3 Let $N = pq$ be an RSA modulus. Assume that we know $\varphi(N)$. Explain how we can recover (in polynomial time) p and q from N and $\varphi(N)$.

4 Prove that RSA works with arbitrary messages (without assuming coprimality with the modulus).

5 *A protocol failure using RSA :* We suppose that Bart has a RSA textbook cryptosystem with a large modulus N for which the factorisation cannot be found in reasonnable time. Suppose that Ralf sends a message to Bart by representing each alphabetic character as an integer between 0 and 25 (i.e., $A = 0$, $B = 1$, etc, not case sensitive!), and then encrypting each single character of the plaintext (i.e., if the word is $HELLO$ then we encrypt H, then E, then L, and so on). Describe how Lisa can easily decrypt a message which is encrypted in this way. Describe a method to prevent this attack.

6 (complementary exercise) *RSA fixed points* : Let $N = pq$ be an RSA modulus with public exponent e and private exponent d. An invertible plaintext M (i.e., with $\gcd(M,N) = 1$ and $0 \leqslant M < N$) is said to be *fixed* if $M^e = M \mod N$. Show that the number of fixed invertible plaintexts is equal to

$$F_{d,N} = \gcd(d-1, p-1) \times \gcd(d-1, q-1)\,.$$

Does the equality $F_{d,N} = \gcd(e-1, p-1) \times \gcd(e-1, q-1)$ also holds? (justify your answswer). What is the possible minimum for $F_{d,N}$? Give at least two invertible plaintexts which are always fixed. What choices of d, p and q could maximise $F_{d,N}$ and the ratio $r_{d,N} = F_{d,N}/$"number of invertible plaintexts"? Could such choice of parameters be dangerous for the security of the system? What do you suggest in order to minimise (or eliminate) such problem?

7 *A Modified RSA cryptosystem* : For $N = pq$, where p and q are distinct odd primes, define

$$\lambda(N) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}\,.$$

Suppose that we modify the RSA cryptosystem by requiring that $ed = 1 \mod \lambda(N)$ (instead of $ed = 1 \mod \varphi(N)$).

(a) Prove that encryption and decryption are still inverse operations in this modified RSA cryptosystem.

(b) If $p = 37$, $q = 79$ and $e = 7$, compute d in this modified RSA cryptosystem, as well as in the original RSA cryptosystem.

8 **On the Wiener's algorithm :** Let N be an RSA modulus and e its public exponent. Suppose that $\frac{a}{b}$ is the convergent of $\frac{e}{N}$ that we are looking (i.e., $\frac{a}{b} = \frac{k}{d}$ in the lectures notations). Show that we can compute the value of $\varphi(N)$ to be

$$\varphi(N) = \frac{(be-1)}{a}\,.$$

From this observation, deduce a simple algorithm in order to check if we found the correct convergent in the Wiener's attack.

9 *Fault analysis on the RSA signature scheme.*
Let $N = pq$ be an RSA modulus with public exponent e and private exponent d. We set $d_p = d \mod (p-1)$ and $d_q = d \mod (q-1)$. Let H be cryptographic hash function whose outputs are integers in the interval $[0, N-1]$. Let M be a message whose signature is

$$s = m^d \mod N,$$

with $m = H(M)$. The signature of the message is verified by computing $m = H(M)$, $m' = s^e \mod N$ and then checking that $m = m'$.
In order to accelerate the signing operations, the signer computes

$$s_p = m^{d_p} \mod p \qquad \text{and} \qquad s_q = m^{d_q} \mod q.$$

(a) Show that the signature s can be computed as $s = as_p + bs_q \mod N$ where a and b are integers satisfying

$$a = \begin{cases} 1 \mod p \\ 0 \mod q \end{cases} \qquad \text{and} \qquad b = \begin{cases} 0 \mod p \\ 1 \mod q. \end{cases}$$

(b) Why this procedure is faster (give an estimate on the gain of speed)?

(c) Suppose that an error occurs during the computation of s_p (i.e., $s_p \neq m^{d_p} \mod p$) and no errors occur during the computation of s_q (i.e., $s_q = m^{d_q} \mod q$). Prove that an adversary who obtains the message representative m and the (incorrect) signature s can easily factor N (i.e., in linear time) and thereafter compute the private exponent d.

(d) Give a simple and effective countermeasure in order to prevent this attack.

10 **A "Multiprimes" version of RSA :** Let r be a fixed positive integer with $r \geq 2$, and $p_1, \ldots, p_r$ distinct odd prime numbers. Set $N = \prod_{i=1}^r p_i$. We will call N the modulus. As the primes are distinct, we have

$$\varphi(N) = \prod_{i=1}^{r} (p_i - 1).$$

Let e be an integer with $1 < e < \varphi(N)$ such that $\gcd(e, \varphi(N)) = 1$. There exists a unique d, with $1 < d < \varphi(N)$, such that $ed = 1 \mod \varphi(N)$. We define, for $x \in \mathbb{Z}/N\mathbb{Z}$, the functions; $E(x) = x^e$ and $D(x) = x^d$.

(a) Show that for all $x \in \mathbb{Z}/N\mathbb{Z}$, we have $D(E(x)) = x$.

(b) Show that we can still apply the broadcast attack seen in the lecture for $e = 3$.

(c) While we can no longer deduce the factorisation of N from the knowledge of $\varphi(N)$ (convince yourself of this claim!), show, heuristically (and following the proof seen in the lectures), that we can still deduce the factorisation of N in (probabilistic) polynomial running time from the knowledge of d (as a preliminary, show that there are 2^r square roots of unity in $\mathbb{Z}/N\mathbb{Z}$). Construct some (realistic) examples in order to test your algorithm.

(d) *Wiener's attack for "Multiprimes" RSA.* For simplicity, assume $r = 3$ and let N be the the "multiprimes" modulus. We suppose that $p_1 < p_2 < 2p_1 < p_3 < 4p_1$ and that $d < \frac{1}{6}N^{\frac{1}{6}}$. Using similar arguments to the proof seen in the lectures, show that given (N, e) we can recover d in linear time. Construct some (realistic) examples in order to illustrate the method. To which value we can extend the bound for d? (perform several experiments in order to support your answer).

(e) Can we perform fault injection on "Multiprimes RSA" as seen in the lectures?

(f) Discuss the interest of the "Multiprimes" RSA (in particular in term of performance using CRT and compared to the classical RSA).