CRITTOGRAFIA 2020/21 – Preappello del 14 dicembre 2020

Esercizio 1 – Numeri Primi

Sia M il proprio numero di matricola, e sia $N = M \bmod 10^4$. Se $N < 2^{10}$, si ponga $N = N + 2^{10}$. Determinare il numero di iterazioni necessarie per eseguire un test di primalità con l'algoritmo di Miller e Rabin, con probabilità di errore minore di $1/N$.

Esercizio 2 – Cifrario di Alberti

Facendo riferimento al seguente allineamento iniziale di un disco cifrante di Alberti

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	1	2	3	4	5
S	D	T	K	B	J	O	H	R	Z	C	U	N	Y	E	P	X	V	F	W	A	G	Q	I	L	M

cifrare il proprio nome e cognome (senza spazi) con il metodo dell'*indice mobile* e con due cambi di chiave.

Esercizio 3 - Curve ellittiche

1. Determinare l'ordine della curva ellittica prima $E_{11}(a,b)$, dove a e b sono le due cifre centrali del proprio numero di matricola.
2. La curva ottenuta definisce un gruppo abeliano? Per quale motivo?

Esercizio 4 – Curve ellittiche

1. Sia M il proprio numero di matricola e sia $k = 2^8 + M \bmod 10^3$. Dato un punto P di una curva ellittica, con quante operazioni (raddoppi e somme di punti) è possibile calcolare il punto $Q = k\,P$? Si discuta brevemente la complessità dell'algoritmo proposto.

2. Dati due punti P e Q appartenenti a una curva ellittica, proporre un semplice algoritmo per il calcolo del logaritmo discreto di Q in base P e discuterne brevemente la complessità.

Esercizio 5 – BB84

Dare un esempio di applicazione del protocollo BB84 (in assenza di crittoanalista sul canale):
- si usi la sequenza di 18 bit ottenuta trasformando in binario ogni cifra decimale del proprio numero di matricola, e prendendo per ciascuna di esse i tre bit meno significativi
- si scelgano a caso le basi per imporre e per misurare la polarizzazione dei fotoni
- si utilizzino 2 bit per effettuare il controllo di eventuali intercettazioni
- si indichi la sequenza finale concordata tra le parti

Esercizio 6 – AES

Sia M il proprio numero di matricola, e sia $N = M \bmod 2^8$.
1. Applicare la S-box del cifrario AES al byte ottenuto rappresentando N in binario.
2. Verificare la non-linearità della S-box sulla coppia di input 00010001 e 11111111.

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

CRITTOGRAFIA 2020/21 – Appello del 9 gennaio 2021

Esercizio 1 – Chiave pubblica

Sia k il numero composto dalle ultime due cifre del proprio numero di matricola. Si consideri il cifrario RSA con chiave pubblica $n = 187$, e con parametro e definito come il più piccolo intero maggiore o uguale a k, idoneo per la definizione del cifrario. **Calcolare** la chiave privata simulando l'algoritmo di Euclide Esteso.

Esercizio 2 – Protocolli a conoscenza zero

Sia P un *prover disonesto* che afferma di essere il proprietario della chiave privata associata alla chiave pubblica $< t, n > = < 110, 187 >$.
Simulare l'esecuzione di due iterazioni del protocollo di Fiat-Shamir, esibendo tutti i valori numerici scambiati, assumendo che:

- Nella prima iterazione P utilizza il numero casuale r composto dalle due cifre centrali del proprio numero di matricola e *correttamente* prevede di ricevere il bit 0 dal verificatore (se $r < 10$, si ponga $r = r + 10$).
- Nella seconda iterazione P utilizza il numero casuale r composto dalle ultime due cifre del proprio numero di matricola e *correttamente* prevede di ricevere il bit 1 dal verificatore (se $r < 10$, si ponga $r = r + 10$).

Esercizio 3 – Curve ellittiche

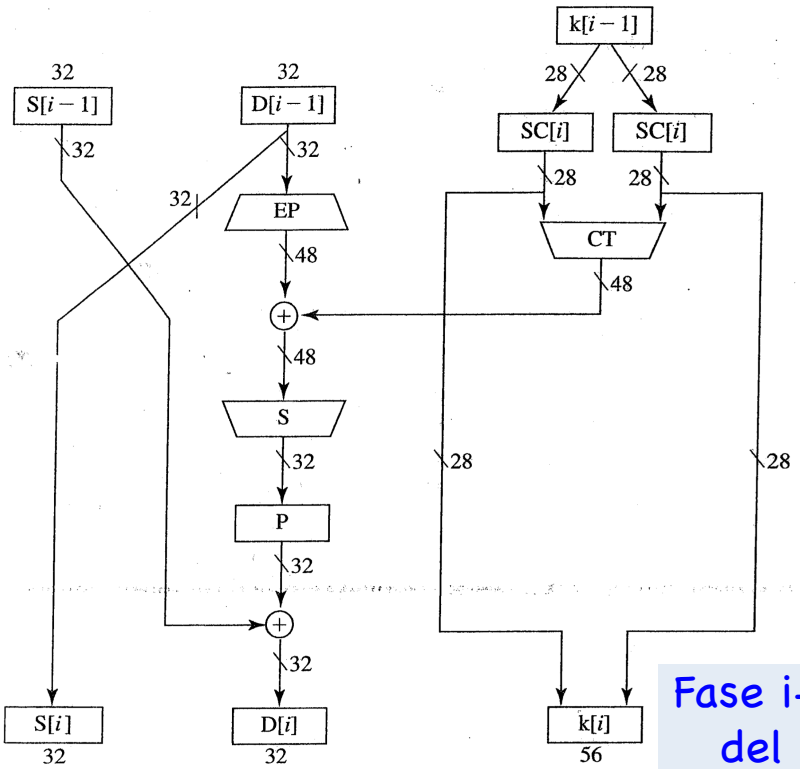
Sviluppare un esempio di applicazione dell'algoritmo di Koblitz per trasformare il messaggio m corrispondente alla cifra meno significativa del proprio numero di matricola in un punto della curva ellittica $E_{23}(1,1)$. Se $m < 5$, si ponga $m = m + 5$.

Esercizio 4 – DES

Sia M il proprio numero di matricola. Si converta M in una sequenza binaria B trasformando in binario ogni cifra decimale di M e prendendo per ciascuna di esse i due bit meno significativi. Nella fase i-esima del DES, B costituisca la **parte finale** della sequenza in ingresso della S-box. **Determinare** il valore degli ultimi 8 bit in uscita dalla S-box, e **indicare** (con interi crescenti tra 1 e 32) la sequenza di posizioni dei bit di $D[i]$ influenzati da B.

Permutazione P

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25



Fase i-esima del DES

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

CRITTOGRAFIA 2020/21 – Appello del 30 gennaio 2021

Esercizio 1 – Cifrari storici

Sia c la cifra decimale di valore maggiore nel proprio numero di matricola, e sia $k = 25 + c$.
Si consideri un cifrario affine in cui si lavora modulo k, e si determini il numero di chiavi possibili. Si scelga infine una chiave e si cifri il proprio cognome.

Esercizio 2 – Scambio di chiavi

L'algoritmo DH per lo scambio pubblico di chiavi è basato sull'uso di un primo p e di un *generatore* g di Z_p^*. Scelti $\boldsymbol{p = 13}$ e $\boldsymbol{g = 2}$:

1. **Verificare** che 2 è un generatore di Z_{13}^*;
2. Presi i due interi *x, y (corrispondenti alle due cifre meno significative* ***e*** *maggiori o uguali a 2 del proprio numero di matricola)* come scelte casuali di due partner che devono costruire una chiave comune, **indicare** come procede l'algoritmo per questi due valori e quale chiave si costruisce.

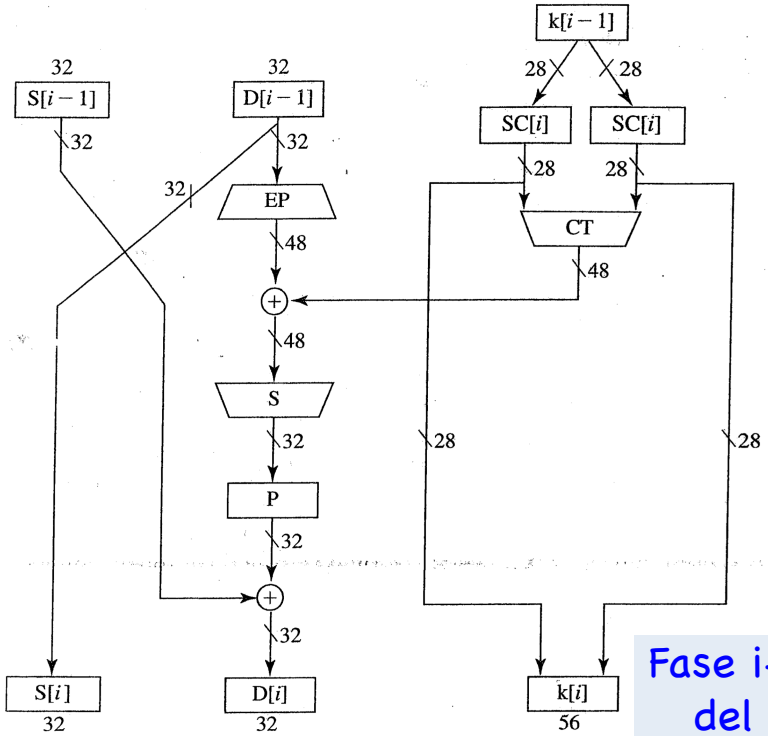
Esercizio 3 – RSA

Sia M il proprio numero di matricola, e sia M' il numero composto dalla prima e dall'ultima cifra di M. Siano quindi p il più piccolo numero primo maggiore di M', e q il numero primo successivo a p. **Costruire** i parametri di un cifrario RSA impiegando p e q scelti sopra. Impiegare l'algoritmo di Euclide Esteso per il calcolo della chiave segreta indicando i calcoli eseguiti.

Esercizio 4 – Protocollo BB84

Dare un esempio di applicazione del protocollo BB84 **(in presenza** di crittoanalista sul canale):

- si usi la sequenza di 18 bit ottenuta trasformando in binario ogni cifra decimale del proprio numero di matricola, e prendendo per ciascuna di esse i tre bit meno significativi
- si scelgano a caso le basi per imporre e per misurare la polarizzazione dei fotoni
- si utilizzino 4 bit per effettuare il controllo delle intercettazioni.



Fase i-esima del DES

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

CRITTOGRAFIA 2020/21 – Appello del 27 marzo 2021

Esercizio 1 – Chiave pubblica

Si consideri il cifrario RSA con chiave pubblica $n = 187$, $e = 9$.
Forzare il cifrario e **decifrare** il crittogramma c composto dalle due cifre centrali del proprio numero di matricola. *Riportare esplicitamente le operazioni aritmetiche eseguite.*

Esercizio 2 – Protocolli a conoscenza zero

Sia P un *prover disonesto* che afferma di essere il proprietario della chiave privata associata alla chiave pubblica $< t, n > = < 155, 187 >$.
Simulare l'esecuzione di due iterazioni del protocollo di Fiat-Shamir, esibendo tutti i valori numerici scambiati, assumendo che:

- Nella prima iterazione P utilizzi il numero casuale r composto dalle ultime due cifre del proprio numero di matricola e *correttamente* preveda di ricevere il bit 1 dal verificatore (se $r < 10$, si ponga $r = r + 10$).
- Nella seconda iterazione P utilizzi il numero casuale r composto dalle due cifre centrali del proprio numero di matricola e *correttamente* preveda di ricevere il bit 0 dal verificatore (se $r < 10$, si ponga $r = r + 10$).

Esercizio 3 – Cifrari storici

Utilizzando la cifratura di Vigenère, cifrare la frase "appello straordinario di crittografia" utilizzando come chiave il proprio cognome.

Esercizio 4 – RSA: attacchi

L'ingenuo Bob usa RSA per ricevere un crittogramma c, corrispondente al messaggio m. La sua chiave pubblica è $< n, e >$, con $n = 55$. Poiché gli sembra uno spreco usare il suo cifrario soltanto una volta, acconsente a decifrare qualunque testo cifrato gli venga inviato, ad eccezione di c, e a rimandare la risposta.
Il malvagio Eve gli invia il testo cifrato $c' = (k^e\, c) \bmod n$, dove k è la cifra meno significativa del proprio numero di matricola (se $k \leq 1$, si ponga $k = 3$).

1. Discutere se il valore di k utilizzato permette a Eve di trovare m.
2. Se necessario, modificare a piacere k in modo da poter condurre l'attacco.
3. Mostrare infine come Eve può risalire a m.