Facultad de Ciencias de la Universidad
Nacional Autónoma de México

Tarea 1 de Criptografía y Seguridad

Parcial 1

Oscar Andrés Rosas Hernandez
Jorge Luís García De Santiago

19 Septiembre 2019

Capítulo 1

Teoría de números

- Supón el siguiente sistema:

$$\begin{aligned} x &\equiv 2 \pmod{22} \\ x &\equiv 4 \pmod{26} \\ x &\equiv 6 \pmod{34} \\ x &\equiv 8 \pmod{46} \end{aligned}$$

Lamentablemente no son coprimos a pares, por lo que no podemos aplicar el TCR (teorema chino del residuo), bueno, no directamente, lo que haremos sera descomponer el modulo de cada uno hasta llegar a un conjunto de ecuaciones que sean coprimas a pares.

Esto sale rápido porque los modulos son 2 veces un primo:

$$\begin{aligned} x \equiv 2 \pmod{22} &\text{ pasará a ser } x \equiv 0 \pmod{2} \text{ y } x \equiv 2 \pmod{11} \\ x \equiv 4 \pmod{26} &\text{ pasará a ser } x \equiv 0 \pmod{2} \text{ y } x \equiv 4 \pmod{13} \\ x \equiv 6 \pmod{34} &\text{ pasará a ser } x \equiv 0 \pmod{2} \text{ y } x \equiv 6 \pmod{17} \\ x \equiv 8 \pmod{46} &\text{ pasará a ser } x \equiv 0 \pmod{2} \text{ y } x \equiv 8 \pmod{23} \end{aligned}$$

Y quitando las repetidamos podemos llegar a un sistema donde los modulos si son coprimos a pares:

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 4 \pmod{11} \\ x &\equiv 4 \pmod{13} \\ x &\equiv 6 \pmod{17} \\ x &\equiv 8 \pmod{23} \end{aligned}$$

Y ahora si:

Entonces $N = (2)(11)(13)(17)(23)$ y $N_1 = (11)(13)(17)(23)$, $N_2 = (2)(13)(17)(23)$, $N_3 = (2)(11)(17)(23)$, $N_4 = (2)(11)(13)(23)$, $N_5 = (2)(11)(13)(17)$, por lo tanto ahora vamos a resolver las congruencias del estilo $c_i\ N_i \equiv a_i \pmod{n_i}$.

- Encontremos a c_1

$$\begin{aligned} c_1(11)(13)(17)(23) &\equiv 1 \pmod 2 \\ c_1(55,913) &\equiv 1 \pmod 2 \\ c_1(1) &\equiv 1 \pmod 2 \\ c_1 &\equiv 1 \pmod 2 \end{aligned}$$

- Encontremos a c_2

$$\begin{aligned} c_2(2)(13)(17)(23) &\equiv 1 \pmod{11} \\ c_2(10,166) &\equiv 1 \pmod{11} \\ c_2(2) &\equiv 1 \pmod{11} \\ c_2 &\equiv 1(6) \pmod{11} \\ c_2 &\equiv 6 \pmod{11} \end{aligned}$$

- Encontremos a c_3

$$\begin{aligned} c_3(2)(11)(17)(23) &\equiv 1 \pmod{13} \\ c_3(8,602) &\equiv 1 \pmod{13} \\ c_3(9) &\equiv 1 \pmod{13} \\ c_3 &\equiv 1(3) \pmod{13} \\ c_3 &\equiv 3 \pmod{13} \end{aligned}$$

- Encontremos a c_4

$$\begin{aligned} c_4(2)(11)(13)(23) &\equiv 1 \quad (\text{mód } 17) \\ c_4(6,578) &\equiv 1 \quad (\text{mód } 17) \\ c_4(16) &\equiv 1 \quad (\text{mód } 17) \\ c_4 &\equiv 1(16) \quad (\text{mód } 17) \\ c_4 &\equiv 16 \quad (\text{mód } 17) \end{aligned}$$

- Encontremos a c_5

$$\begin{aligned} c_5(2)(11)(13)(17) &\equiv 1 \quad (\text{mód } 23) \\ c_5(4,862) &\equiv 1 \quad (\text{mód } 23) \\ c_5(9) &\equiv 1 \quad (\text{mód } 23) \\ c_5 &\equiv 1(18) \quad (\text{mód } 23) \\ c_5 &\equiv 18 \quad (\text{mód } 23) \end{aligned}$$

Por lo tanto una solución x_0 es:

$$\begin{aligned} x_0 =& \sum_{i=0}^{r} a_i N_i c_i \\ =& a_1 N_1 c_1 + a_2 N_2 c_2 + a_3 N_3 c_3 + a_4 N_4 c_4 + a_5 N_5 c_5 \\ =& \\ & 2((11)(13)(17)(23))1+ \\ & 2((2)(13)(17)(23))6+ \\ & 4((2)(11)(17)(23))3+ \\ & 6((2)(11)(13)(23))16+ \\ & 8((2)(11)(13)(17))18 \\ =& 1668658 \quad (\text{mód } (2)(11)(13)(17)(23)) \\ =& 1668658 \quad (\text{mód } 111,826) \\ =& 103094 \quad (\text{mód } 111,826) \end{aligned}$$

Ahora, todas las soluciones van a ser módulo $(2)(11)(13)(17)(23)$ es decir $103094 \ (\text{mód } 111,826)$.

Por lo tanto tenemos soluciones que son congruentes módulo 111,826, es decir $103094, 1780484, \ldots 111,826k + 103094$

- Demostremos que las leyes de los signos en $\mathbb{Z}_n$ funcionan.

  Sea $a, b \in \mathbb{Z}_n$ entonces:

  - $(a)(-b) = -(ab) \in \mathbb{Z}_n$
    Por definicion $-(ab)$ es una solucion a la ecuacion $ab + x = 0$ ahora veamos que pasa si decimos que $x = a(-b)$, entonces sustituyendo tenemos que $ab + a(-b) = a[b + (-b)] = a(0) = 0$. Entonces $a(-b) = -(ab)$.
  - $(-a)(b) = -(ab) \in \mathbb{Z}_n$
    Por definicion $-(ab)$ es una solucion a la ecuacion $ab + x = 0$ ahora veamos que pasa si decimos que $x = (-a)b$, entonces sustituyendo tenemos que $ab + (-a)b = [a + (-a)]b = (0)b = 0$. Entonces $(-a)b = -(ab)$.
  - $(-a)(-b) = (ab) \in \mathbb{Z}_n$
    Vamos a usar las anteriores tenemos que $(-a)(-b)$ y podemos decir que $x = -b$, y reescribir como $(-a)x$ y usando los anteriores podemos decir que $-(ax)$ es decir $-[a(-b)]$ ahora tambien usando las anteriores tenemos que $a(-b) = -(ab)$, es decir $-[a(-b)] = -[-(ab)]$ ademas sabemos que el inverso de un numero y del inverso es el mismo numero y, por lo tanto $-[-(ab)] = ab$.

- Encontrar una raíz primitiva de $\mathbb{Z}_7$.

  Recordemos que dado un número natural n, decimos que a es una raíz primitiva módulo n, si a genera como grupo a $\mathbb{Z}_n^*$, es decir, si $\forall b \in \mathbb{Z}_n^*$ existe $k \in \mathbb{Z}_n$ tal que $a^k \equiv b(mod\ n)$.

Por pura fuerza bruta podemos llegar a una solución:

$$\begin{aligned}
3^1 &= 3 &&= 3 \pmod 7\\
3^2 &= 9 &&= 2 \pmod 7\\
3^3 &= 27 &&= 6 \pmod 7\\
3^4 &= 81 &&= 4 \pmod 7\\
3^5 &= 243 &&= 5 \pmod 7\\
3^6 &= 729 &&= 1 \pmod 7
\end{aligned}$$

Por lo que 3^{algo} genera a todos los elementos de $\mathbb{Z}_7^*$ (todo $\mathbb{Z}_7$ sin contar al cero).

Capítulo 2

Cesar - Shift cipher

Podemos hacer dos cosas, por un lado usar los progamas que hicimos en laboratio y usar fuerza bruta para ir probando cada una de las 26 llaves posibles (decimos que son 26 porque no aparece la ñ en el texto) o podemos hacer un poco de analisis, por ejemplo viendo que la J se repite mucho como una letra sola, por lo que podemos suponer que $e_k(y) = J$ es decir que $k = 11$.

Con esto logramos ver este mensaje tan bonito:

HOLA MUCHACHOS ESPERAMOS QUE EN ESTA SU PRIMER TAREA LA DISFR- UTEN Y NO LA SUFRAN (RECUERDEN QUE ESTAN AQUI PORQUE ASI LO DEC- IDIERON). LA DEDICACION Y EL TRABAJO QUE HASTA ESTE MOMENTO

HAN REFLEJADO EN LAS CLASES, NOS HACE PENSAR QUE LLEGARAN MUY LEJOS, POR FAVOR NO SE DETENGAN.

TRABAJAN EN EQUIPOS PARA HACER MEJOR Y MAS RAPIDO LAS COSAS, ASI QUE NO SEAN UNA CARGA PARA SUS EQUIPOS DEJANDO QUE LOS DEMAS HAGAN TODO NI TAMPOCO SEAN LOS PROTAGONISTAS, ESCUCHEN EL PUNTO DE VISTA DE SU COMPANERO Y LUEGO DETERMINEN QUE ES LO QUE MAS LE CONVIENE AL EQUIPO YA SABEN A LO QUE NOS REFERIMOS, QUE SU MOTIVACION SEA LO MEJOR PARA EL EQUIPO.

ESTA TAREA ES PURA Y MERA FORMALIDAD NO LA PLANEAMOS PARA QUE SEA EL RETO DEL SIGLO O ALGO ASI, NOS INTERESA QUE HAGAN LO BASICO PERO QUE LO HAGAN BIEN. POR CIENRO ULTIMAMENTE ES ESTA CLASE SE ESTA CARACTERIZAN- DO PORQUE SUS COMPANEROS ANTERIORES HAN PUESTO EMPENO EN APRENDER MAS DE LO QUE PIDE EL TEMARIO Y ESO NOS LLAMA LA ATENCION PERO A LA VEZ ES DE ESPERARSE YA QUE ESTAMOS EN LA UNIVERSIDAD AUTONOMA DE MEXICO Y REALMENTE LLEGAN MUY BUENOS ALUMNOS. LOS ALENTAMOS A QUE INVESTI- GUEN EN INTERNET COSAS NUEVAS QUE LES ABRA MAS EL PANORAMA QUE SEAN AMBICIOSOS Y NO SE QUEDEN SOLO CON LO LA CLASE PARA ESO SI DEBEN USAR

TODOS SUS RECURSOS, POR FAVOR NO LO HAGAN SOLO PARA CUMPLIR CON LA TAREA Y HACER

ASI SU MENOR ESFUERZO NO LO NECESITAN PARA LO QUE SI LO NECES- ITAN ES PARA BUSCAR INNOVACIONES AL RESPECTO Y LLEVARLAS A

LA REALIDAD ES UNA OBLIGACIO NS ES DE SU INTERES LA CRIPTOGRAFIA Y QUE NADIE LES DIGA QUE TODO ESTA ESCRITO O QUE NO PUEDEN, A USTEDES LES TOCA LOS CAMBIOS DE TECNOLOGIA DONDE TENDRAN QUE HACER USO DE TODOS SUS CONOCIMIENTOS PARA REALIZAR LOS NUEVOS DESAFIOS.

NUESTRA META ES SOLO ENCAMINARLOS AL INICIO DE LA CRIPTOGRAFIA. ASI QUE EN VEZ DE TOMAR DOS ARRANQUES DE DESESPERACION, POR FAVOR TOMENSE DOS TASAS DE SU BEBIDA PREFERIDA Y TRABAJEN

CON TIEMPO. SIN MAS POR EL MOMENTO NOS DESPEDIMOS Y LES RECO- RDAMOS DISFRUTEN EL CURSO.

Capítulo 3

Vigenére

Lo primero que hay que hacer es buscar patrones repetidos, una vez teniendo eso podremos analizar la secuencia, posición, distancia y factores. Para esto haremos un programa que nos ayude con dicha tarea. Ahora bien, se hizo un script en Python para encontrar patrones repetidos y así facilitarnos la tarea, como se nos dio la pequeña pista de que la clave era al menos de longitud cinco decidimos buscar coincidencias de esa longitud y sus múltiplos. Teniendo en cuenta eso, se mostrará el programa para encontrar las apariciones:

```
s =
    'FUDPBVEQAHKEYECSUQWSKMBPFVIPDQNAETSPLMUOEUXIOFDQRWGNOXOUHQCCVAPDEWEQCZQSXXPTOESSEAXR
    '
def parse_pos_a_distancias(l):
    s = ''
    ln = len(l)
    for i in range(ln - 1):
        n = l[i + 1] - l[i]
        s += str(n)
        if i < ln - 2:
            s += ', '
    return s


start = 5
end = 20
l = len(s)

d = dict()
for i in range(start, end):
```

```
    for k in range(l - i):
        aux = s[k:k + i]
        if aux not in d:
            d[aux] = [k]
        else:
            d[aux].append(k)

for (k, v,) in d.items():
    if len(k) % 5 == 0 and len(v) > 3:
        print('secuencia: {}, longitud: {}, posicion: {}, distancia:
   {}, factores:'.format(
            k, len(k), ','.join(map(str, v)),
   parse_pos_a_distancias(v)))
```

Capítulo 4

Hill