ENCRIPTADOR DE TRANSACCIONES

INTEGRANTES

- **SERGIO HERNANDO BARON RIVERA 2201885**
- **MATEO GERONIMO ORTIZ CRUSATE 2201778**
- **CARLOS ALBERTO BARRERA CADENA 2202047**

Programa

1. Introduccion
2. Datos
3. Metodo
4. Resultados
5. Conclusiones

INTRODUCCION

Un banco planea implementar nuevos cajeros en sus principales sucursales para esto contrata unos ingenieros de sistemas que busquen la manera mas segura de proteger la base de datos de los cajeros automáticos.

La información que contienen estos cajeros no suele estar del todo segura, se propone mejorar esto haciendo uso de métodos de encriptación, de esta manera garantizar la seguridad y privacidad de la información de los usuarios que utilizen el cajero y sentirse seguros usando el mismo.

DATOS

Haremos uso de los siguientes datos los cuales fueron obtenidos algunos de una base de datos de un banco generico y los datos restantes fueron creados a partir de un algoritmo propio:

Obtenidos de la base de datos

- Numero de identificación (id)
- Tipo de transacción (ingreso-retiro)
- Monto de la transacción

Generados a partir del algoritmo

- Fecha
- Balance

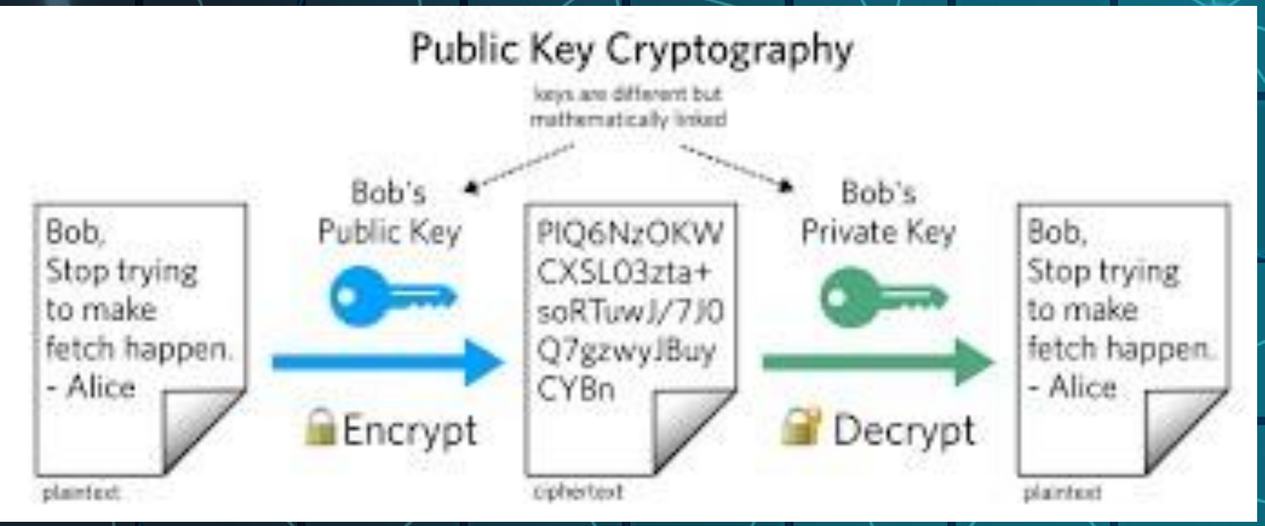
METODO

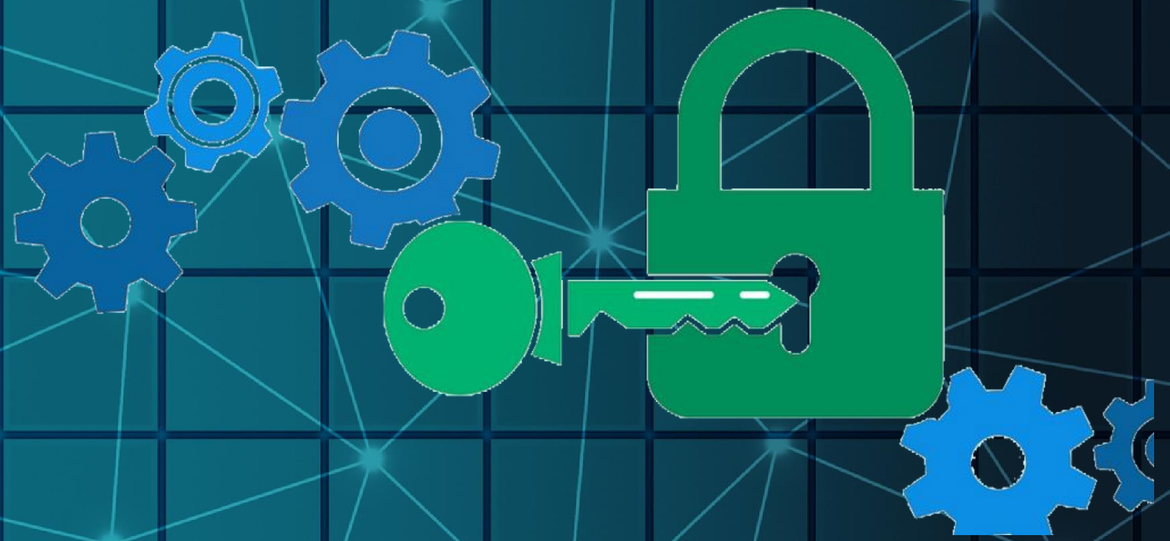
Creamos un algoritmo en python que nos permita encriptar las distintas tuplas que asignamos y separamos anteriormente de la base de datos, los elementos dentro de estas tuplas serán divididas en dos tipos:

- Elementos únicamente numéricos.
- Elementos alfanuméricos.

ELEMENTOS NUMERICOS

Estos elementos únicamente numéricos son Monto y Balance serán encriptados usando el método de RSA, este sistema al encriptar nos proporciona dos tipos de "llaves", la llave de cifrado sera publica mientras que la llave de descifrar sera completamente privada y única.





ELEMENTOS ALFANUMERICOS

El numero de identificación y la fecha serán encriptados usando la variante 256 del método SHA(secure hashing algorithm), este método nos permite transformar un conjunto arbitrario de datos, en un valor único de longitud fija de 64 caracteres, lo que nos permitirá que los datos sean lo suficientemente seguros.

RESULTADOS

Como se ilustra en la primera imagen tenemos los elementos de las transacciones bancarias.

- Datos sin encriptar

	Numero de ID	Fecha	Tipo de transaccion	Monto	Balance
0	a78884f5e76951188c1e719d4956773a	11-10-2018	retiro	350	451
1	b0333294fef6ff1299102a70ad46b126	24-06-2021	retiro	202	303
2	7b8d2a2780adae0cd0c248e92c1b28dc	20-11-2018	ingreso	291	22
3	cc4abaa500f7db4390ae3f02bd36d805	13-10-2021	retiro	214	225
4	cc4abaa500f7db4390ae3f02bd36d805	3-10-2021	retiro	45	65
5	5f0c29acdcb1bddba271984d4a351445	3-04-2018	retiro	15	20
6	5f0c29acdcb1bddba271984d4a351445	31-03-2020	retiro	19	76
7	5c4e2e4d68b9e8d3c5fc0107bd82f271	5-10-2019	ingreso	385	32
8	a6f1e3793969ffd44588b58f40a5307b	24-08-2019	ingreso	70	21
9	132e4663b9d5e1b28e02b35717ce18ce	9-03-2018	retiro	116	230
10	cd45d14a750b28bc2b0b0288f75a4c62	7-01-2021	retiro	163	325
11	d378d0b0ade20c73c868f5431d4b4ef8	4-12-2018	retiro	74	645
12	bdba4fb350c131eabd16942fbec8445a	6-10-2021	ingreso	30	604
13	dc879d41982dfa14abb14d96818eadd2	18-06-2021	retiro	157	250
14	c270235846c2104dfb7d0fc57298f6ff	3-11-2019	ingreso	233	253
15	ce8150cf1461297516d4f65d8258a36b	25-01-2019	ingreso	125	460
16	ea589a947c4c128a6c6b81fb35605d40	25-04-2018	retiro	215	525
17	a8f1ba811701cef72fb2d7bc0d000965	9-04-2021	ingreso	30	286
18	60a06917fcdfc145734fb27b496fdd07	6-04-2020	ingreso	75	607
19	0a82c36cadf8fd68800c905af515758c	24-09-2020	ingreso	284	189

Aqui se muestran los datos ya encriptados con sus respectivos metodos

- Datos encriptados

	A	B	C	D	E	F
1	Numero de ID	Fecha	Tipo de Transaccion	Monto	Balance	
2	c91c92ad454de26f01001f82451ddd4bf82	5a61ebc32862c678d10cc8e425ecf5421b6	5	b'z+\x12\xc7\x95/M\xc8d\t\x13\x9a\xe1	b'\x89\xac\x98O\xd1\xc6\x8bF(\xf5<\xaeZ\x84\x	
3	3728e397225ec9a619261d7d4ee96f2df0a	02c54652334883d7e2c3979a795fd5b4087	16	b"\x80\x98\xaa\x9e\xe1\xc4;7\xfc\xc7\	b"\x18\x07\xf6\x84q\xa1\x9cU\xf6\xbd\xf8\xc5\	
4	2ec99190cb2b2af55515e1baf599e493194	49d3e37e312e199554198713cbbb9449d3	24	b"\x07q\xd3[\xb5\xc0\xd2\x0cB\xb6(Bv	b'$\x04D\xe0\xb3Kn\x9dWy&\x8a\x16d\xddA5\r	
5	258e6e72dc14eb08a8b43cfe3be615d958	2ff6890144362d0e4fa2ee758ca703c86fab	38	b"U\xcd\xe2w\xcd\xec:aPZY\x1a68\xc6\	b'.]!\xd6\x0fa\xd8Q:\x87x\xb5\xf0u\x87\x95\xc2	
6	22ef0a93c9538da356fb2667adec93e07b3	c0c9c01e59824f6826649769e21d486db99	49	b"D\xdd\xe8\x826\x1e'\xd8^\xae\xd1N	b"i\xae\x81\xde\xca\x14\xcdt\xe0m\x98\x8c4\x	
7	0c3f3b6370054189b2bdbbf58367abbd2d	d66df412a00ada492f703d078e9e1016c85	60	b"\\\x1b'~\xb1\xaa\xd6}\xc9\x93]-\xff\	b'\x07.\xc3/\xa7*\x19y\x0c\xdd\xc4\x85\x84\x90	
8	7bb5e6b4ff3d8659cec97edd0eff315fed3	5905f1799c160e6b31e32698000ad0c5ee2	71	b')fH\x13\x85\x05\xb8\x01\xc7\xd7kb<\	b'sR\x8b\x14\xc34\x94\xb7s\x02i\xb5\xc7\x81[Y\	
9	b2f62e29602312b32eb4bdeab312f9bddd	8b8228806866b5b3d02c6936a05b93ce105	79	b'g<\x88\xc8?\xcb\xf32J \xaeQ\x8b<\x(	b'I^\x14K\xb2\x02\xd0yLW~\x07(y\xd9\xdbF\xba	
10	bc43aad7af25a82f69a77eff3affb784f25cc	f202357ef19d3c0909d7985b83572710d13	90	b'Z\x86@\xc5rf4\xc2\x14\xda\xce\xd7\	b'^\x07\xd9\xe8\x1f\x0e\x90!\x7f\xd6X\x12c,O\	
11	1018b24bab818d36112cfcf6506c68a8a87t	6a7b8655bc1a90e0dd40097e7aa9194022	104	b'\x8f\xb5T\xccK\xfaR\x1d\x16`a\x91R \	b'4.\x98\x16\xa4pn\x0b\xcf\xaa4\x00\xecN*\x12	
12	b391f476d063137146d7829f69a575f703f8	0d6ac51d17ae0d77bdf69036745f16a9808	115	b'XI\xa2\x89hm\x7f\x83\r3@G\x1d@\x1	b'{\xf1]1\xcf\xe7\xc1\xa5\xa1\xa1+\xca w)\xdb\	
13	039ccfd790362c688343722d9a92cc05e751	28f82fa9a586d6269aec1e374fb844c6f4d9	126	b'+r\x01_\x9c*\xfbc\xbe!\xf1\xeb\x03\	b"\x13o|6\x1c\xc8\xb0\xa5\x03`\xaaD+e\xc1^\xe	
14	945195281ce2f459291bbaf8900b6480e84	6ab38f69ea24f57b3f58db5cca815a913275	134	b'6a\x1f\xa0[\xbbZC\x07\xfe\x03\xe8\x	b'.\x8c\xb4\xfb\xea\x8e\xbed\x8bV@_\x06*\xf4	
15	a36947fc627f199212239334308584fcf1714	04afeb16288fdd7ba182d4b5ee4128cf5c1	148	b'7\xa0\x19T\xbf\xb3\xb5\xa8\x0c-|u\\	b'h\xdcU\xa3\x19_Eq2\xbd\x04\x88^k\xe7\x15\x	
16	87db88b70bc49aedf4cbb407ec6ac7ceb7t	9c022a0d5e053d64ff0b4f8c4a8720f9b6b2	156	b'\x81]\xc9\x00k.,T\xe1Q\x98\xfe\x0b\	b's'"~\x88\\5\xae\xe9A\xf0\x84\xc1<\r+\x857\xc6	
17	d05eb5303e15325506867ec0927d65e235:	aeda0160ba87c9a700d681be780a9602f8a	167	b'\tU\x01A\xcc\x0fF\xff\xb1]\xbb\x0f$\	b'^\xad2J\xcd[6\xa9\xa7\xa8\x87\xe5\x01\xe3\x	
18	5f17057af2c2412007da0cba8bfe77dfee65	adde255efa4885042d43469161592a5139f	181	b'(\x8d[\x0f$\x9c*\x1e\x94\x1c\xf7\xf1	b'\x0b\x8ax\xd2y\xabB\x17\xeb\xe4\x0b=\x03\x	
19	54b43c6e4d4a97d5b055863494c2d5a440€	8f777c81170a11e30c8bec33ce8f666894b0	189	b'=U\xa6\xe2T\x08\xb4g\xbd\x92\xca=;'	b"\x06\xfa\xc2\xed\xd3\x13\x1c\x16\xe27a\x11(	
20	88178629c758e7784834d5200ff4325a568	38f67db7e713ccf5e2e2aa24d9d70a64646	200	b'\x84\xeeR\xd5\xda\x9f\xb8\x1a\x88\	b'\x15 ^x\x8d\x04\x1eF\xb2\xb9!?'\\=\x93\xae`\x	
21	94840eb007bd0b433c8b3d1ceb47bf5d97	0738e2c2d623a81acbefa35bd36e6e7c6dc	211	b'e\xaa\xd6\xfc\xf4<R\xac\xf7\x8eD\xc	b"W\xcd\xf37\x82'\x19\x9e;\x1d;b\x92b\x140\x1	
22						
23						

CONCLUSIONES

- Se encriptarón los datos numericos usando el metodo RSA de manera satisfactoria .
- Se cifraron los datos alfanumericos usando el método SHA256 exitosamente.
- En definitiva se consiguio importar los datos de un documento excel y exportarlos nuevamente a un nuevo archivo.
- Se aumentó la seguridad y privacidad de los datos de la base de datos de transacciones bancarias digitales.