COMPUTING BASICS, CRYPTO, BLOCK CHAIN AND CLOUD COMPUTING

DATA BASICS

- All digital computers operate on a binary basis
- Essentially, the most basic form of information is either:
  - On or Off
  - 1 or 0
- This basic piece of information is called a bit

DATA BASICS

- Data bits are generally organized in 8 bit blocks known as bytes
  - A byte can have a value of 2^8 different values (256 different values)
  - 0 0 0 0 0 0 0 0 = 0
  - 0 0 0 0 0 0 0 1 = 1
  - 0 0 0 0 0 0 1 0 = 2
  - 0 0 0 0 0 0 1 1 = 3
  - 0 0 0 0 0 1 0 0 = 4
  - ....
  - 1 1 1 1 1 1 1 1 = 255

DATA BASICS

- Data bits are generally organized in 8 bit blocks known as bytes
  - While we learn in base 10, computers operate in base 16
  - 11111111=255=FF

Decimal (Base 10)	Binary (Base 2)	Hexadecimal (Base 16)
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

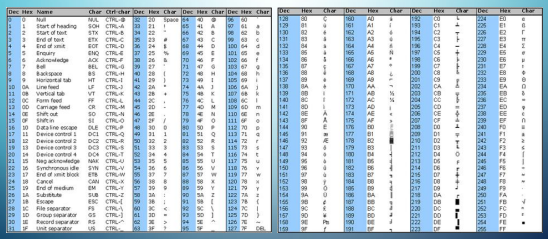
DATA BASICS

- Data bits are generally organized in 8 bit blocks known as bytes
  - While we learn in base 10, computers operate in base 16
  - 11111111=255=FF

DATA BASICS

- To make data consistent, in 1963 the American Standard Code for Information Interchange arrived at an 8 bit representation of letters numbers and characters
  - ASCII characters
  - The ASCII standard is common for European based alphabets
  - Other languages may use other character sets (such as CCCII for Chinese characters)

DATA BASICS

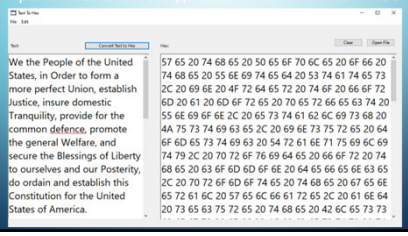


Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	(space)	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	φ
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	Pts	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

DATA BASICS

- This is important because unencrypted data is often stored in ASCII Hex format



DATA BASICS

- This is important because most, if not all, data can be read in Hex format

DATA BASICS

- Knowing that data is stored in numbers and interpreted in standard ways is a basic for having exchangeable and usable data and essentially transforms data to information

DATA BASICS

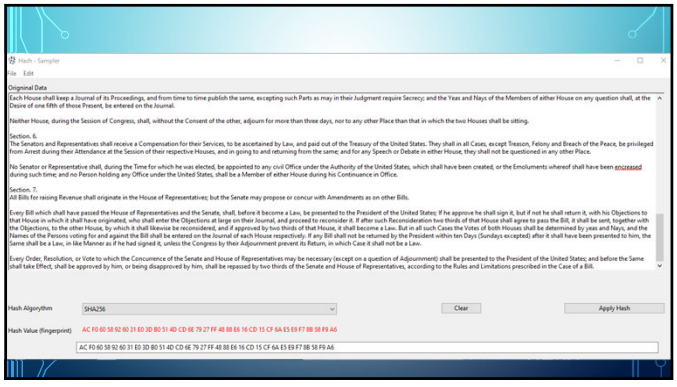
- Because data is essentially a string of numbers, mathematical calculations can be run against the data, including mathematical functions to create a unique "fingerprint" for data.
- These functions to create "fingerprints" are called hashes

HASH

- A hash is generally an algorithm or function that converts data into a specific length of data using a common formula or algorithm.
- It essentially maps any size of data down to a fixed length of data
- It does so exactly the same way every time
- Therefore, the resulting fixed length string of data is unique, but reproducible for each set of data it is run against

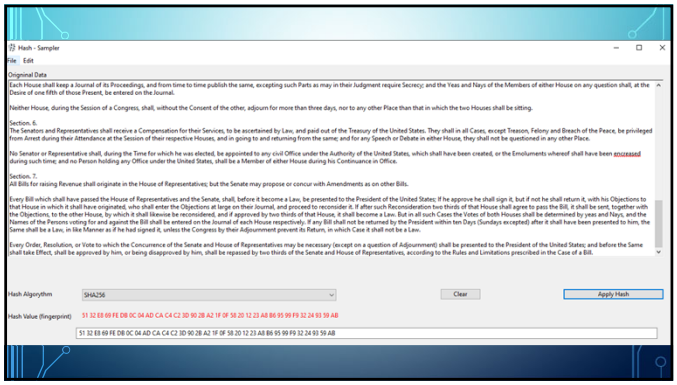
HASH

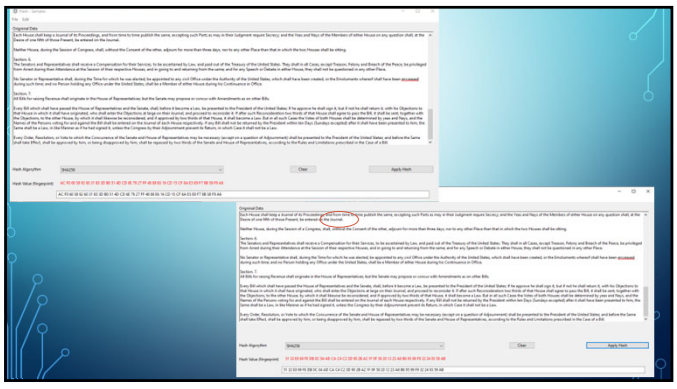
- There are several public hash functions that can be used against any set of data
  - MD5
  - SHA1
  - SHA256
  - SHA512



HASH

- If even one number is out of place or changed, the HASH function will return a different Hash value





HASH

- The keys to a workable Hash function are:
  - It always return the same value for the same information
  - It is quick to compute
  - It always returns values of the same length
  - It Can be applied to input of any length
  - It is so robust that it is infeasible that two different inputs could result in the same hash value

HASH

HASH

- The value of a Hash function is that it can tell you if a file has been altered from its form when the initial hash function was run

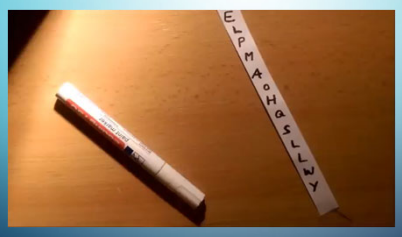
ENCRYPTION

- A hash function can let you know if a file or data have been altered or corrupted, but it doesn't actually protect the data or information
- Encryption provides such protection

ENCRYPTION

- Encryption has been used to protect sensitive information for eons

ENCRYPTION



- https://youtu.be/KJpYA7pyFwQ

ENCRYPTION

- Substitution Encryption
  - Substituting one value for another
  - For example changing each letter in a message to a character that is 4 numbers higher in the ascii table than the original character
    - "THIS CLASS IS BORING" becomes XLMWGPEWWMWFSVMRK. The "T" in this is transformed to the character 4 characters higher which is "X", the "H" in this text is transformed to the character 4 characters higher which is "L", and so on.
  - The famed "enigma machines of WWII worked this way.

ENCRYPTION

- https://youtu.be/QwQVMqfoB2E

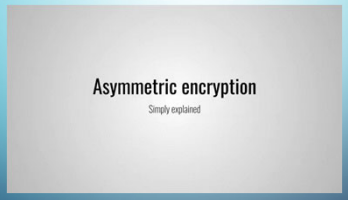
ENCRYPTION

- Substitution Encryption
  - Substitution can be effective, but it is often subject to weaknesses if someone determines or obtains the keys or algorithm

ENCRYPTION

- Asymmetric Encryption
  - Asymmetric Encryption is another encryption method that uses two keys (rather than a single, even if complex, key).
  - This a modern and sophisticated encryption technique. Asymmetric key encryption integrates two cryptographic keys for implementing data security.
  - These keys are identified as a "Public Key" and a "Private Key." The "public key", as the name implies, is accessible to all who want to send an encrypted message.
  - The other is the "private key" that is kept secure by the owner of that public key or the one who is encrypting.

ENCRYPTION



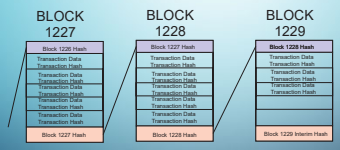
- https://youtu.be/AQDCe585Lnc

BLOCK CHAIN

- Using Hash and Encryption
  - Transactions are encrypted and stored on a ledger
  - Each transaction has a hash to fingerprint the original information in the transaction
  - When a determined number of transactions and hashes are recorded, the block of those transactions also receives a hash, which is then incorporated into the next block
  - If any block is tampered with, the hash will no longer pass verification
  - In this way, blocks are chained together and, once recorded, may not be altered without immediate detection of corruption

BLOCK CHAIN

- Using Hash and Encryption

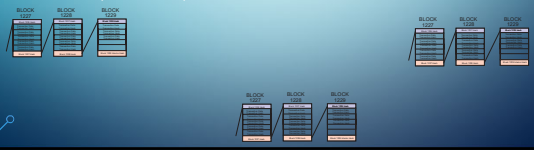


BLOCK CHAIN

- Distributed ledgers
  - To add additional integrity, some block chain implementations use multiple ledgers to keep duplicate data in remote locations to further enhance the security of the information
  - If a solution is found to alter a transaction within a block without initial detection, it will still fail to match the hashes in duplicate blocks distributed through the network and thus be exposed as corrupted or altered

BLOCK CHAIN

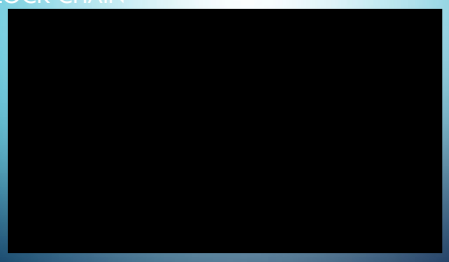
- Distributed ledgers
  - To add additional integrity, some block chain implementations use multiple ledgers to keep duplicate data in remote locations to further enhance the security of the information
  - If a solution is found to alter a transaction within a block without initial detection, it will still fail to match the hashes in duplicate blocks distributed through the network and thus be exposed as corrupted or altered



BLOCK CHAIN

- https://youtu.be/3xGLc-zz9cA

BLOCK CHAIN



- https://youtu.be/ID9KAnkZUjU

BLOCK CHAIN - CRYPTOCURRENCY

- Because Block Chain can be distributed and is immutable, it is a format for record keeping of financial transactions
- BITCOIN is the most popular Block Chain Crypto Currency

BLOCK CHAIN – BITCOIN

- https://youtu.be/M_zCjjy59cg

BLOCK CHAIN – BITCOIN

- Do cryptocurrencies, like Bitcoin change the gambling analysis of any of the following:
  - Lotteries
  - Games of Chance
  - Sports Wagers
  - Bookmaking

CLOUD COMPUTING

- In short, using someone else's computers to store, process, collect or report data or data processing functions

CLOUD COMPUTING

- Cloud computing allows businesses to outsource the core IT functions of a company
  - By using shared resources, a company can reduce IT budgets, enhance security, and scale as needs require
  - There are many different forms of cloud computing

CLOUD COMPUTING

- https://youtu.be/uroryFU78gM

CLOUD COMPUTING

- Cloud computing leverages the scale of large scale cloud computing providers to allow flexible sharing of resources
  - AMAZON
  - GOOGLE
  - IBM
  - MICROSOFT
  - ORACLE
  - … and others

CLOUD COMPUTING

- https://youtu.be/p7MqvJAKLoM

CLOUD COMPUTING

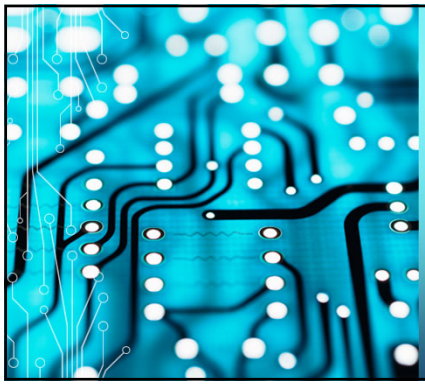
- One key element of cloud computing is load balancing
  - Load balancing is the seamless use of multiple global data centers to provide services to cloud computing customers

CLOUD COMPUTING

- https://youtu.be/h8EqM6Xt3MA

CLOUD COMPUTING

- How does cloud computing enter the gambling analysis of any of the following:
  - Lotteries
  - Games of Chance
  - Sports Wagers
  - Bookmaking



QUESTIONS