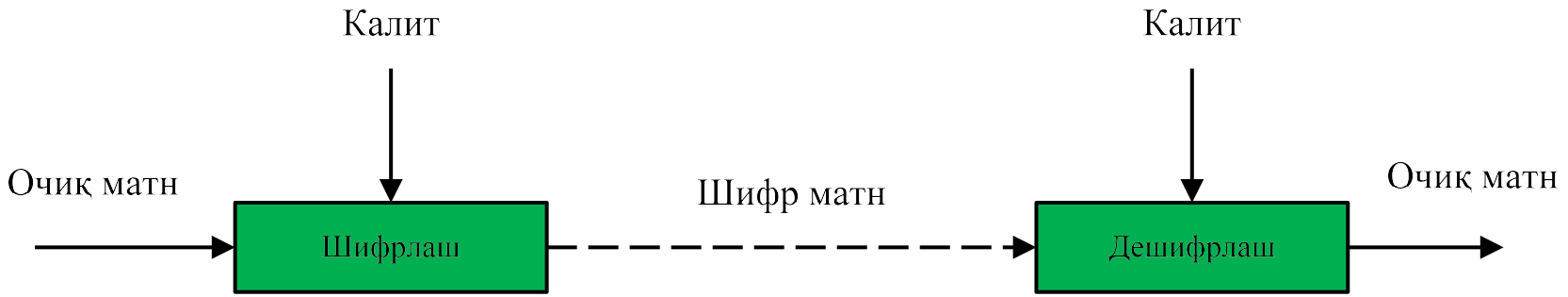
5-Маъруза: Криптографиянинг асосий тушунчалари ва тарихи

Криптографиянинг асосий тушунчалари

- ***Криптология*** - “махфий кодлар”ни яратиш ва бузиш фани ва санати;
- ***Криптография*** – “махфий кодлар”ни яратиш билан шуғулланади;
- ***Криптотаҳлил*** – “махфий кодлар”ни бузиш билан шуғулланади;
- ***Крипто*** – юқоридаги тушунчаларга (ҳаттоки бунданда ортиғига) синоним бўлиб, контекст маъносига кўра фарқланади.

Криптографиянинг асосий тушунчалари

- ***Шифр*** ёки ***криптотизим*** маълумотни ***шифрлаш*** учун фойдаланилади. Ҳақиқий шифрланмаган маълумот ***очиқ матн*** деб аталиб, шифрлашнинг натижаси ***шифрматн*** деб аталади. Ҳақиқий маълумотни қайта тиклаш учун шифрматнни ***дешифрлаш*** зарур бўлади. ***Калит*** криптотизимни шифрлаш ва дешифрлаш учун созлашда фойдаланилади.



Криптографиянинг асосий тушунчалари

Шифрлаш ва дешифрлаш масалаларига тегишли бўлган, маълум бир ***алфавитда*** тузилган маълумотлар ***матнларни*** ташкил этади. ***Алфавит*** - ахборотни ифодалаш учун фойдаланиладиган чекли сондаги белгилар тўплами. Мисоллар сифатида:

- ўттиз олтита белгидан (ҳарфдан) иборат ўзбек тили алфавити;
- ўттиз иккита белгидан (ҳарфдан) иборат рус тили алфавити;
- йигирма саккизта белгидан (ҳарфдан) иборат лотин алфавити;
- икки юзи эллик олтита белгидан иборат ASCII компьютер белгиларининг алфавити;
- бинар алфавит, яъни 0 ва 1 белгилардан иборат бўлганалфавит;
- саккизлик ва ўн олтилик саноқ системалари белгиларидан иборат бўлган алфавитларни келтириш мумкин.

Криптографиянинг асосий тушунчалари

- ***Симметрик*** шифрларда маълумотни шифрлаш ва дешифрлаш учун бир хил калитдан фойдаланилади.
- Бундан ташқари ***очиқ калитли*** **(*ассиметрик*)** криптотизимлар мавжуд бўлиб, унда шифрлаш ва дешифрлаш учун турлича калитлардан фойдаланилади.
- Турли калитлардан фойдаланилгани боис, *шифрлаш калитини* **ошкор қилса бўлади** ва шуни учун ***очиқ калитни криптотизим деб аталади***.
- Очиқ калитини криптотизимларда шифрлаш калитини ***очиқ калити*** деб аталса, дешифрлаш калитини ***шахсий калит*** деб аталади.
- Симметрик калитли криптотизимларда эса калит - ***симметрик калит*** деб аталади.

Керкхофс принципи

- **Идеал шифрлар** учун калитсиз шифрматндан очиқ матнни тиклашнинг имкони бўлмаслиги зарур.
  - Бу шарт, ҳаттоки ҳужумчилар учун ҳам ўринли.
- Ҳужумчи алгоритм (шифрлаш алгоритми) ҳақида барча маълумотларни билган тақдирда ҳам **калитсиз** очиқ матнни тиклашнинг имкони бўлмаслиги зарур.
  - Ушбу қўйилган мақсад, амалда бундан фарқди бўлиши мумкин.
- Криптографиянинг фундаментал назариясига кўра криптотизимнинг **ички ишлаш принципи** ҳужумчига тўлиқ ***ошкор бўлиши*** зарур.
- Ҳужумчига фақат криптотизимда фойдаланилган **калит *номаълум*** бўлиши зарур.
- Бу таълимот ***Керкхофс принципи*** деб аталади.

Кодлаш ва шифрлаш орасидаги фарқ

- Аксарият ҳолларда фойдаланувчилар маълумотни ***шифрлаш*** ва ***кодлаш*** тушунчаларини бир хил деб тушунилади.
  - Аслида эса улар икки турлича тушунчалардир.
- ***Кодлаш*** – маълумотни осонгина қайтариш учун ҳаммага (ҳаттоки ҳужумчига ҳам) очиқ бўлган схема ёрдамида маълумотларни бошқа форматга ўзгартиришдир.
- Кодлаш маълумотлардан фойдаланиш қулайлигини таъминлаш учун амалга оширилади ва ҳамма учун очиқ бўлган схемалардан фойдаланилади.
- Масалан, *ASCII, UNICODE, URL Encoding, base64*.

ASCII кодлаш стандарти

Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char	Dec	Hex	Oct	Binary	Char
0	00	000	0000000	NUL (null character)	32	20	040	0100000	space	64	40	100	1000000	@	96	60	140	1100000	`
1	01	001	0000001	SOH (start of header)	33	21	041	0100001	!	65	41	101	1000001	A	97	61	141	1100001	a
2	02	002	0000010	STX (start of text)	34	22	042	0100010	"	66	42	102	1000010	B	98	62	142	1100010	b
3	03	003	0000011	ETX (end of text)	35	23	043	0100011	#	67	43	103	1000011	C	99	63	143	1100011	c
4	04	004	0000100	EOT (end of transmission)	36	24	044	0100100	$	68	44	104	1000100	D	100	64	144	1100100	d
5	05	005	0000101	ENQ (enquiry)	37	25	045	0100101	%	69	45	105	1000101	E	101	65	145	1100101	e
6	06	006	0000110	ACK (acknowledge)	38	26	046	0100110	&	70	46	106	1000110	F	102	66	146	1100110	f
7	07	007	0000111	BEL (bell (ring))	39	27	047	0100111	'	71	47	107	1000111	G	103	67	147	1100111	g
8	08	010	0001000	BS (backspace)	40	28	050	0101000	(	72	48	110	1001000	H	104	68	150	1101000	h
9	09	011	0001001	HT (horizontal tab)	41	29	051	0101001	)	73	49	111	1001001	I	105	69	151	1101001	i
10	0A	012	0001010	LF (line feed)	42	2A	052	0101010	*	74	4A	112	1001010	J	106	6A	152	1101010	j
11	0B	013	0001011	VT (vertical tab)	43	2B	053	0101011	+	75	4B	113	1001011	K	107	6B	153	1101011	k
12	0C	014	0001100	FF (form feed)	44	2C	054	0101100	,	76	4C	114	1001100	L	108	6C	154	1101100	l
13	0D	015	0001101	CR (carriage return)	45	2D	055	0101101	-	77	4D	115	1001101	M	109	6D	155	1101101	m
14	0E	016	0001110	SO (shift out)	46	2E	056	0101110	.	78	4E	116	1001110	N	110	6E	156	1101110	n
15	0F	017	0001111	SI (shift in)	47	2F	057	0101111	/	79	4F	117	1001111	O	111	6F	157	1101111	o
16	10	020	0010000	DLE (data link escape)	48	30	060	0110000	0	80	50	120	1010000	P	112	70	160	1110000	p
17	11	021	0010001	DC1 (device control 1)	49	31	061	0110001	1	81	51	121	1010001	Q	113	71	161	1110001	q
18	12	022	0010010	DC2 (device control 2)	50	32	062	0110010	2	82	52	122	1010010	R	114	72	162	1110010	r
19	13	023	0010011	DC3 (device control 3)	51	33	063	0110011	3	83	53	123	1010011	S	115	73	163	1110011	s
20	14	024	0010100	DC4 (device control 4)	52	34	064	0110100	4	84	54	124	1010100	T	116	74	164	1110100	t
21	15	025	0010101	NAK (negative acknowledge)	53	35	065	0110101	5	85	55	125	1010101	U	117	75	165	1110101	u
22	16	026	0010110	SYN (synchronize)	54	36	066	0110110	6	86	56	126	1010110	V	118	76	166	1110110	v
23	17	027	0010111	ETB (end transmission block)	55	37	067	0110111	7	87	57	127	1010111	W	119	77	167	1110111	w
24	18	030	0011000	CAN (cancel)	56	38	070	0111000	8	88	58	130	1011000	X	120	78	170	1111000	x
25	19	031	0011001	EM (end of medium)	57	39	071	0111001	9	89	59	131	1011001	Y	121	79	171	1111001	y
26	1A	032	0011010	SUB (substitute)	58	3A	072	0111010	:	90	5A	132	1011010	Z	122	7A	172	1111010	z
27	1B	033	0011011	ESC (escape)	59	3B	073	0111011	;	91	5B	133	1011011	[	123	7B	173	1111011	{
28	1C	034	0011100	FS (file separator)	60	3C	074	0111100	<	92	5C	134	1011100	\	124	7C	174	1111100	|
29	1D	035	0011101	GS (group separator)	61	3D	075	0111101	=	93	5D	135	1011101	]	125	7D	175	1111101	}
30	1E	036	0011110	RS (record separator)	62	3E	076	0111110	>	94	5E	136	1011110	^	126	7E	176	1111110	~
31	1F	037	0011111	US (unit separator)	63	3F	077	0111111	?	95	5F	137	1011111	_	127	7F	177	1111111	DEL

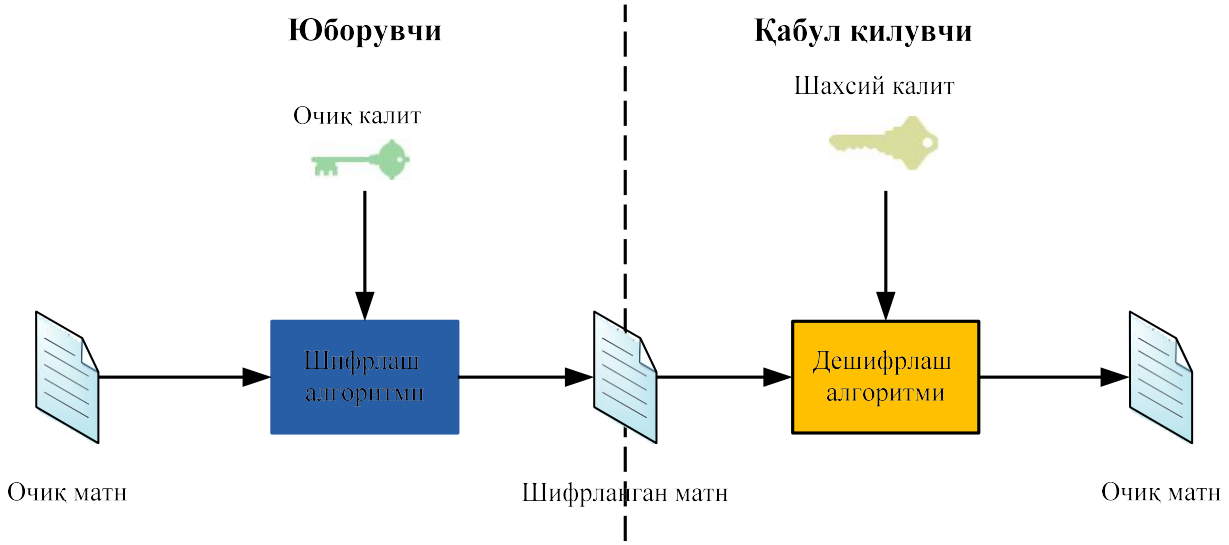
Шифрлаш

- ***Шифрлаш*** – жараёнида ҳам маълумот бошқа форматга ўзгартирилади, бироқ уни фақат махсус шахслар (дешифрлаш калитига эга бўлган) қайта ўзгартириши мумкин бўлади.
- ***Шифрлашдан асосий мақсад*** маълумотни **махфийлигини** таъминлаш бўлиб, уни қайта ўзгартириш баъзи шахслар (дешифрлаш калитига эга бўлмаган) учун чекланган бўлади.

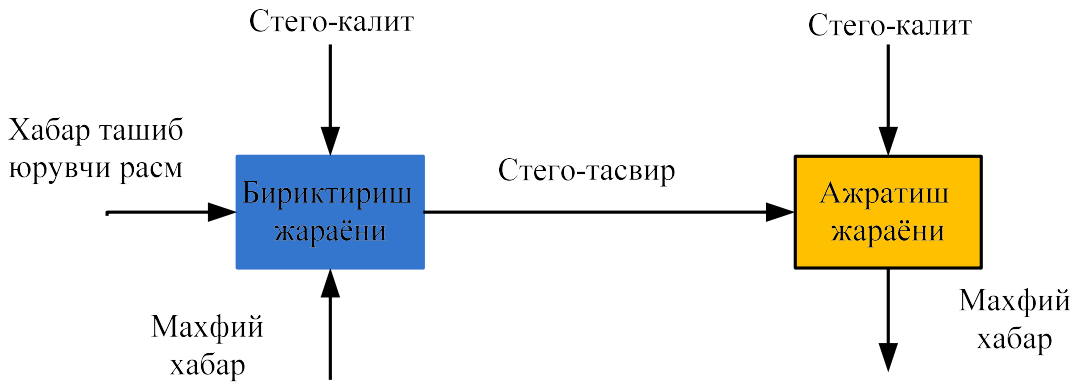
Криптография ва стеганография

- ***Стенанография*** – бу ***махфий хабарни сохта хабар*** ичига беркитиш орқали алоқани яшириш ҳисобланади.
- Бошқа сўз билан айтганда стеганографиянинг асосий ғояси – ***бу махфий маълумотларнинг мавжудлиги ҳақидаги шубҳани олдини олиш*** ҳисобланади.
- ***Криптография***да эса жўнатувчи фақат очиқ матн кўринишидаги хабар юбориши мумкин, бунда у хабарни очиқ тармоқ (масалан, Интернет) орқали узатишдан олдин шифрланган матнга ўзгартиради. Ушбу шифрланган хабар қабул қилувчига келганида эса яна оддий матн кўринишига қайтарилади.
- Умумий ҳолда маълумотни ***шифрлашдан асосий мақсад*** (симметрик ёки очиқ калитли криптографик тизимлар асосида фарқи йўқ) – **маълумотни махфийлигини қолганлардан сир тутиш**дир.

Криптография ва стеганография



а) Криптографик ҳимоя



б) Стеганографик ҳимоя

Криптографиянинг асосий бўлимлари

1. ***Симметрик калитли криптография.***
   - Маълумотни шифрлашда ва дешифрлашда ягона калитдан (симметрик калитдан) фойдаланилади.
   - Шунинг учун ҳам симметрик калитли криптотизимларни – *бир калитли* криптотизимлар ҳам деб юритилади.
   - Бундан келиб чиқадики, симметрик калитли шифрлаш алгоритмларидан фойдаланиш учун ҳар иккала томонда бир хил калит мавжуд бўлиши зарур.
2. ***Очиқ калитли криптография***
   - маълумотни шифрлаш қабул қилувчининг *очиқ калити* билан амалга оширилса, уни дешифрлаш қабул қилувчининг *шахсий калити* билан амалга оширилади.
   - Шунинг учун ҳам очиқ калитли криптотизимларни – *икки калитли* криптотизимлар деб ҳам юритилади.

Криптографиянинг асосий бўлимлари

3. Хеш функциялар

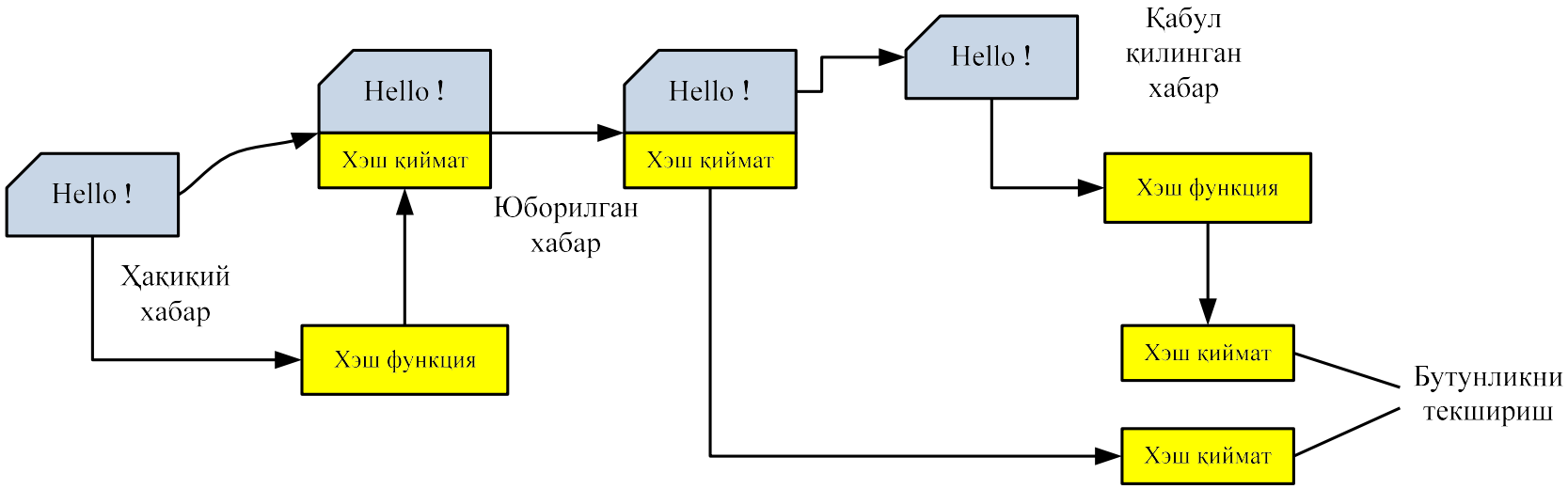
- Маълумотни хэшлаш унинг **бутунлигини кафолатлаш** мақсадида амалга оширилиб, агар маълумот узатилиш давомида ўзгаришга учраса, у ҳолда уни аниқлаш имкони мавжуд бўлади.
- Хэш-функцияларда одатда *кирувчи маълумотнинг ўзгарувчан* бўлиб, *узунлиги чиқишда ўзгармас* қайтаради. *узунликдаги* қийматни
- Замонавий хэш функцияларга MD5, SHA1, SHA256, O‘z DSt 1106:2009 ларни мисол келтириш мумкин.
- Қуйида “*hello*” хабарини турли хэш функциялардаги қийматлари келтирилган:
  - $MD5(hello) = 5d41402abc4b2a76b9719d911017c592$
  - $SHA1(hello) = aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d$
  - $SHA256(hello) = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e7304336$
    $2938b9824$

Криптографиянинг асосий бўлимлари

3. *Хеш функциялар*

- Хеш функция қуйидаги хусусиятларга эга:
  - Бир хил кириш ҳар доим бир хил чиқишни (*хэш қиймат* деб аталади) тақдим этади.
  - Бир қанча турли киришлар бир хил чиқишни тақдим этмайди.
  - Чиқиш қийматдан кирувчи қийматни ҳосил қилишнинг имконияти мавжуд эмас (бир томонламалик).
  - Кириш қийматини ўзгариши чиқишдаги қийматни ҳам ўзгаришига олиб келади.
- Одатда хэш функциялар киришда маълумотдан ташқари хеч қандай қийматни талаб этмагани боис, ***калитсиз криптографик функциялар*** деб ҳам аталади.

Хеш функция асосида маълумот бутунлигини текшириш



- Бунга асосан юборувчи хабарнинг хэш қийматини ҳисоблайди ва уни қабул қилувчига хабар билан биргаликда юборади. Қабул қилувчи дастлаб хабарнинг хэш қийматини ҳисоблайди ва қабул қилинган хэш қиймат билан солиштиради. Агар ҳар иккала хэш қиймат тенг бўлса, у ҳолда маълумотнинг бутунлиги ўзгармаган, акс ҳолда ўзгарган деб топилади.

Криптографик акслантиришлар

- Одатда криптографияда маълумотларни шифрлашда (дешифрлашда) қуйидаги икки турдаги ***акслантириш***лардан фойдаланилади.
  - Улардан бири ***ўрнига қўйиш (substitution)*** акслантириш бўлса, иккинчичи ***ўрин алмашиш (permutation)*** акслантиришидир.

Ўрнига қўйиш акслантириши

- Ўрнига қўйиш акслантиришида, очиқ матн белгилари бир алфавитдан олиниб, унга мос шифрматн бошқа бир алфавитдан олинади.

Очиқ матн	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Шифрматн	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Содда кўринишда олинган ўрнига қўйиш акслантириши асосида шифрлаш учун олинган матн қуйида келтирилган. Ушбу содда шифрлаш усули **Цезар** номи билан машҳур.
- Масалан, агар очиқ матн “**HELLO**” га тенг бўлса, унга мос ҳолда шифрматн “**KHOOR**” га тенг бўлади.
- Мазкур ҳолда шифрматн алифбоси очиқ матн алифбосидан 3 га суриш натижасида ҳосил қилинган ва шунинг учун **шифрлаш калитини 3** га тенг деб қараш мумкин.

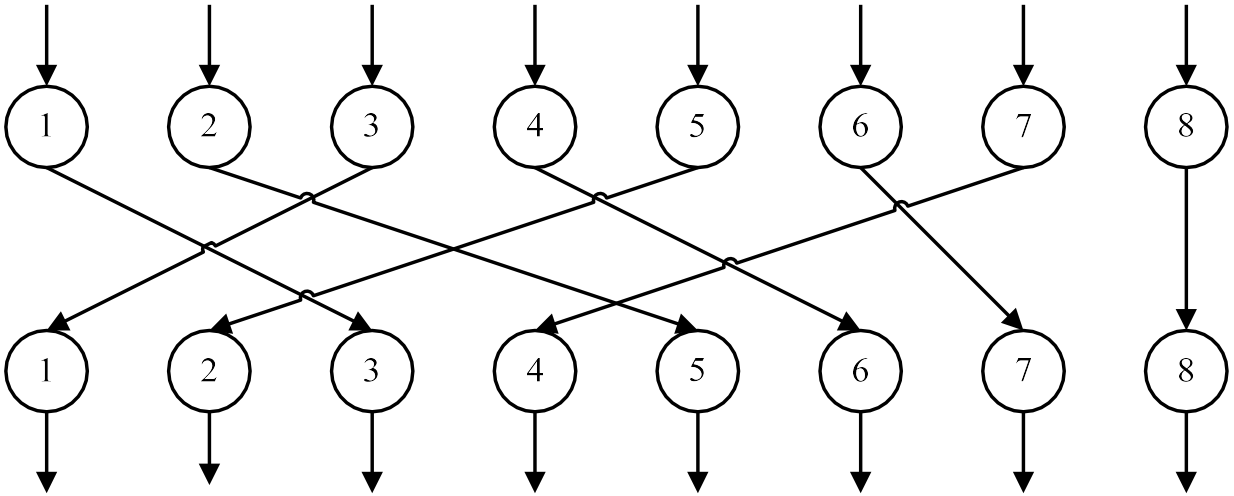
Ўрнига қўйиш акслантириши

- Ўрнига қўйиш акслантиришида **очиқ матндаги белгилар** шифрматнда **бўлмаслиги мумкин**.
- Бироқ, очиқ матндаги белгиларнинг **такрорланиш частотаси** шифрматндаги белгиларда ҳам **бир хил бўлади** (кўп алифболи ўрнига қўйиш усуллари бундан мустасно).
- Масалан, юқоридаги мисолда очиқматндаги “L” ҳарфининг такрорланиш частотаси 2 га тенг. Унинг ўрнига қўйилган шифрматндаги “O” ҳарфининг ҳам такрорланиш частотаси 2 га тенг. Бу ҳолат очиқматндаги қолган белгилар учун ҳам ўринли.

Ўрин алмаштириш акслантириши

- **Очиқ матн белгиларининг ўрни** бирор қоидага кўра **ўзаро алмаштирилади**. Бунда очиқ матнга иштирок этган белгилар шифрматнга ҳам иштирок этиб, фақат уларнинг ўрни алмашган ҳолда бўлади.

Очиқ матн = “POSSIBLE”



Шифр матн = “SIPLOSBE”

Криптографиянинг тарихи

- Маълумотларни шифрлашнинг дастлабки кўринишларидан минг йиллар аввал фойданиб келинган.
- Яқин ўн йилликларга қадар фойдаланилган шифрларни - ***классик*** шифрлар деб аталган.
- Баъзи манбаларда ҳисоблаш қурилмалари яратилгунга қадар фойдаланилган шифрлар – ***классик шифрлар*** даврига тегишли деб олинган. Ундан кейинги давр эса ***замонавий шифрлар*** даври деб юритилади.

Криптографиянинг тарихи

1. ***Қадимий давр (қадимий давр классик шифрлари).*** Ушбу давр классик шифрлари асосан бир алфавитли ўрнига қўйиш ва ўрин алмаштириш акслантиришларига асосланган. Уларга мисол тариқасида **Цезар, Полибия** квадрати усулларини келтириш мумкин.
2. ***Ўрта давр (ўрта давр классик шифрлари).*** Ушбу давр шифрлари асосан кўп алифболи ўрнига қўйишга асосланган бўлиб, уларга **Вижинер, Атбаш** усулларини мисол келтириш мумкин. Ушбу давр шифрлари биринчи давр шифрларига қараганда юқори бардошликка эга бўлган.

Криптографиянинг тарихи

3. ***1 ва 2 – жахон уриши даври (1 ва 2- жахон уриши даври классик шифрлари).*** Ушбу давр криптотизимлари асосан электромеханикага асосланган бўлиб, радиотўлқин орқали шифрматнни узатишни (морзе алифбоси) амалга оширган. Мазкур даврга оид шифрлаш усулларига **Zimmermann телеграми, Энигма шифри, SIGABA** машиналарини мисол келтириш мумкин.
4. ***Компьютер даври (замонавий шифрлар).*** Ушбу давр шифрлари ҳисоблаш қурилмаларига мўлжалланган бўлиб, юқори хавфсизлик даражасига эга ҳисобланади. Замонавий шифрларга мисол сифатида **DES, AES, ГОСТ 28147-89, IDEA, A5/1, RC4 (барчаси симметрик) ва RSA, Эл-Гамал (очиқ калитли)** ларни келтириш мумкин.

Бир мартали блокнот

- **Бир мартали блокнот (one time pad)** ёки **Вернам** шифри номи билан танилган криптотизим ***бардошли*** шифрлаш алгоритми ҳисобланади.
- Бир мартали деб аталишига асосий сабаб, ундаги ***калитнинг (блокнотнинг)*** **бир марта** фойдаланилиши.
- Шунинг учун ҳам *амалга ошириш жуда ҳам мураккаб*.
- Мисол тариқасида қуйидаги бинар кодлаш жадвали олинсин.

Белгилар	E	H	I	K	L	R	S	T
Бинар қиймат	000	001	010	011	100	101	110	111

H	E	I	L	H	I	T	L	E	R
001	000	010	100	001	010	111	100	000	101

Бир мартали блокнот

- Бир мартали блокнот усулида шифрлаш учун ***очиқ матн узунлигига тенг бўлган тасодифий танланган калит*** зарур бўлади.
- Очиқ матнга калитни XOR амалида қўшиш орқали **шифрматн ҳосил қилинади** (*P – очиқ матн, K – калит* ва *C – шифрматн* деб белгиланса): $C = P \oplus K$.
- **XOR амали ($\oplus$):**

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Дешифрлаш учун: $P = C \oplus K$, яъни, $P = C \oplus K = P \oplus K \oplus K = P$.

Мисол 1

- Юқорида келтирилган очиқ маттнишифрлаш учун қуйидаги калит олинган бўлсин:

111	101	110	101	111	100	000	101	110	000

- Ушбу калит асосида **шифрлаш** қуйидагича амалга оширилади:

	H	E	I	L	H	I	T	L	E	R
Очиқ матн:	001	000	010	100	001	010	111	100	000	101
Калит:	111	101	110	101	111	100	000	101	110	000
Шифрматн:	110	101	100	001	110	110	111	001	110	101
	S	R	L	H	H	H	T	H	S	R

Мисол 1

- **Дешифрлаш** учун:

	S	R	L	H	H	H	T	H	S	R
Шифрматн:	110	101	100	001	110	110	111	001	110	101
Калит:	111	101	110	101	111	100	000	101	110	000
Очиқ матн:	001	000	010	100	001	010	111	100	000	101
	H	E	I	L	H	I	T	L	E	R

Бир мартали блокнот: Ценарий 1

- А томонинг душмани Т мавжуд ва у А томон калит сифатида қуйидагини фойдаланган деб уйлайди:

101	111	000	101	111	100	000	101	110	000

- Мазкур ҳолатда душман Т ушбу калитни Б томонга юбора олса, у ҳолда Б томон қуйидаги очиқ матнга эга бўлади:

	S	R	L	H	H	H	T	H	S	R
Шифрматн:	110	101	100	001	110	110	111	001	110	101
“Калит”:	101	111	000	101	111	100	000	101	110	000
“Очиқ матн”:	011	010	100	100	001	010	111	100	000	101
	K	I	L	L	H	I	T	L	E	R

- Агар Б томон ***криптографиядан хабари бўлмаса***, у ҳолда А томон учун **жиддий муаммо** туғилади.

Бир мартали блокнот: Ценарий 2

- А томон душмани Т томонидан қўлга олинди ва у шифрматнни ҳам билади ва А томондан калитни талаб қилмоқда. А томон ҳар иккала томон учун ҳам “ўйнашиши” айтади ва калитни қуйидагича тенг дейди:

111	101	000	011	101	110	001	011	101	101

- Т томон эса қуйидаги очиқ матнга эга бўлади:

	S	R	L	H	H	H	T	H	S	R
Шифрматн:	110	101	100	001	110	110	111	001	110	101
“Калит”:	111	101	000	011	101	110	001	011	101	101
“Очиқ матн”:	001	000	100	010	011	000	110	010	011	000
	H	E	L	I	K	E	S	I	K	E

- Агар Т томон криптографияданхабаридбўлмаса, очиқ матнга ишонади ва А томонни қўйиб юборади.

Бир мартали блокнот

- Кафолатга эга эмаслиги сабабли, ушбу келтирилган мисоллар бир мартали блокнот шифрини ***бардошли*** эканини кўрсатади. Яъни, турли калит учун турлича очиқ матнни олиш мумкин.
- Агар калит *бир марта фойдаланилса*, ҳужумчи **очиқ матнни топа олмайди**.
- Шифрматнга қараб фақат *очиқ матн узунлигини билиши* мумкин.
- Агар **битта калитдан кўп марта фойдаланилса**, у ҳолда **жиддий хавфсизлик муаммоси** туғилади!!!!

Мисол 2

- Фараз қилайлик, қуйидаги икки очиқ матн P_1 ва P_2 битта калит K дан фойдаланиб шифрланган: $C_1 = P_1 \oplus K$ ва $C_2 = P_2 \oplus K$.
- Криптографияда ушбу ҳолатни “**хавфлилик**” деб аталади.
- Яъни, фойдаланилган калит энди муаммо туғдирмайди:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

- Икки матн ва калит қуйидагига тенг бўлсин:

$$P_1 = LIKE = 100\ 010\ 011\ 000$$
$$P_2 = KITE = 011\ 010\ 111\ 000$$
$$K = 110\ 011\ 101\ 111$$

Мисол 2

- У ҳолда шифрланган матнлар қуйидагича бўлади:

	L	I	K	E
P_1:	100	010	011	000
K:	110	011	101	111
C_1:	010	001	110	111
	I	H	S	T

	K	I	T	E
P_2:	011	010	111	000
K:	110	011	101	111
C_2:	101	001	010	111
	R	H	I	T

- Агар ҳужумчи криптогарфияни яқиндан билса ва битта калитдан фойдаланилганини билса:
  - 2 ва 4 шифрматн белгилари тенг эканлигини осонгина топа олади.
- Бундан ташқари, ҳужумчи тахминий P_1 очиқ матн олиб уни тўғрилигини P_2 очиқ матн билан текшириб кўриш имкониятига эга.

Мисол 2

- Агар $P_1 = KILL$ = 011 010 100 100 бўлса,

	K	I	L	L
Тахминий P_1:	011	010	100	100
C_1:	010	001	110	111
Тахминий K:	001	011	010	011

- Олинган калит K ёрдамида эса иккинчи шифрматндан очик матнни хисоблайди:

C_2:	101	001	010	111
Тахминий K:	001	011	010	111
Тахминий P_2:	100	010	000	100
	L	I	E	L

- Топилган калит иккинчи очиқ матн учун мос бўлмагани сабабли, тахминий P_1 ни нотўғрилигини билади.
- У қачонки $P_1 = LIKE$ шаклида тахмин қилса, у ҳолда $P_2 =$ $KITE$ ни ва калитни топа олади.

Кодлар китоби

- Кодлар китоби луғатга ўхшаш китоб бўлиб, **(очиқ матн сўзлари)** ва унга мос бўлган **код сўзлардан (шифрматн)** ташкил топган.
- Қуйида биринчи жахон уришида Немислар томонидан фойдаланилган ко келтирилган:

Очиқ матн	Шифрматн
Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
⋮	⋮

- Масалан, “Februar” сўзини шифрлаш учун бутун сўз 5-белгили код сўз 13605 билан алмаштирилган.

Кодлар китоби

- Ушбу кодлар китоби орқали машҳур Zimmermann телеграмини шифрланган.
- 1917 йилда биринчи жахон уриши даврида, Германия ташқи ишлар вазири Артур Зиммерман Германиянинг Мексикадаги элчисига шифрланган кўринишдаги телеграм юборади.
- Шифрланган хабар Британияликлар томонидан тутиб олинади.
- Бу вақтда Британия ва Франция Германия билан урушаётган ва АҚШ эса бетараф ҳолатда эди.

Зиммерман телеграми

Зиммерман телеграми - дешифрланган

We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.

Signed, ZIMMERMANN

Кодлар китоби

- Кодлар китоби асосида шифрлаш **ўрнига қўйиш акслантиришига** асосланган.
- Кодлар китоби ҳозирда амалда қўлланилувчи **симметрик блокли шифрларни яратишга** асос бўлган (улар билан кейинги дарсда танишиб чиқилади).
- Кодлар китоби **ўз даврида етарли хавфсизликни таъминлаган** шифрлаш усули ҳисобланади.

ЭЪТИБОРИНГИЗ УЧУН
РАХМАТ!!!