



Page NO.

1. 1 to 20 – Mid Term
2. 21 to 52- Final Term

MD IFTAKHAR KABIR SAKUR

25th BATCH

COMPUTER AND COMMUNICATION ENGINEERING

International Islamic University Chittagong

COURSE CODE: CCE-4825

COURSE TITLE: Cryptography and Network Security

COURSE TEACHER:

Ahmad

Lecturer
ETE

Q8

[Cryptography & Network Security]

Cipher Text :-

- Replace each letter in Alphabet with the letter standing three places further down the alphabet.
- For each plaintext letter 'p' substitute the ciphertext letter 'c':

$$C = \text{Cipher Text} = (P+K) \bmod 26 = \text{Encryption}$$

$$P = \text{Plain Text} = (C-K) \bmod 26 = \text{Decryption}$$

Example:-

K=3
 Encrypt "Neso Academy" using Cipher Text

plain Text:-

N E S O A C A D E M Y

Encryption:-

$$N = (13+3) \bmod 26 = 16 = \text{P}$$

$$E = (4+3) \bmod 26 = 7 = \text{H}$$

$$S = (18+3) \bmod 26 = 21 = \text{V}$$

$$O = (14+3) \bmod 26 = 17 = \text{R}$$

$$A = (0+3) \bmod 26 = 3 = \text{D}$$

$$C = (2+3) \bmod 26 = 5 = \text{F}$$

$$\begin{aligned} A &= 13 = \text{G} \\ D &= (3+3) \bmod 26 = 6 = \text{G} \\ E &= (4+3) \bmod 26 = 7 = \text{H} \\ M &= (12+3) \bmod 26 = 15 = \text{P} \\ Y &= (24+3) \bmod 26 = 1 = \text{B} \end{aligned}$$

Encryption standard & padding rule

• Cipher Text :- G H V R D F D G C H P B T

Decryption process

G H V R D F D G C H P B

$$G = (16 - 3) \text{ mod } 26 = 13 = \text{M}$$

$$H = (17 - 3) \text{ mod } 26 = 14 = \text{O}$$

$$V = (21 - 3) \text{ mod } 26 = 18 = \text{S}$$

$$R = (17 - 3) \text{ mod } 26 = 14 = \text{O}$$

$$D = (3 - 3) \text{ mod } 26 = 0 = \text{A}$$

$$F = (5 - 3) \text{ mod } 26 = 2 = \text{C}$$

$$D = \text{A}$$

$$G = (6 - 3) \text{ mod } 26 = 3 = \text{D}$$

$$H = (7 - 3) \text{ mod } 26 = 4 = \text{E}$$

$$P = (15 - 3) \text{ mod } 26 = 12 = \text{M}$$

$$B = (1 - 3) \text{ mod } 26 = -2 \Rightarrow 24 = \text{Y}$$

$$\therefore \text{NBSO} \quad \text{ACADEMY}$$

$$R = E = 13 = \text{M}$$

$$A = Q = 17 = \text{R}$$

$$T = S = 19 = \text{S}$$

Brute Force on Ceaser cipher:-

PlayFair:-

→ Diagram

→ Ignore Repeating letter in matrix.

→ Same column \rightarrow wrap around.

→ Same row \rightarrow wrap around.

→ Rectangle \Leftrightarrow swap [IF 1,2 condition is not working]

PlainText:- Attack

A	F	e	K	B
D	E	F	G	H
I	J	L	M	N
P	Q	R	S	U
V	W	X	Y	Z

also if plain!.. Balloon

Diagram Balloon

Diagnaph:- At ta ck

Encrypted:- tc

Keyword:- Monarchy

plainText:- Instruments

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

M	O	N	A	P	R	E
C	H	Y	B	D		
(Q)	F	(G)	(H)	K		
L	P	Q	R	S	T	Z
U	V	W	X	Z		

plainText:- Instruments

↓↓↓↓↓ → filler letter

Diagraphs In st ru me nt sz

→ filling words

Decryption

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

→ of if i have

→ o k b e

Hill Cipher

Encryption process:- $(PK) \bmod 26$ (pay) $\rightarrow (239)$

Decryption process:- $PXKXK^T \bmod 26$

Example:-

Encrypt "pay more money" using Hill cipher

Key

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{bmatrix}$$

Solution:-

PlainText:-

$$\begin{bmatrix} p & a & y & m & o & r & e & m & o & n & e & y \\ \downarrow & \downarrow \\ 15 & 0 & 24 & 12 & 14 & 17 & 4 & 12 & 14 & 13 & 4 & 24 \end{bmatrix} \rightarrow (15 \ 0 \ 24 \ 12 \ 14 \ 17 \ 4 \ 12 \ 14 \ 13 \ 4 \ 24)$$

Here : matrix 3×3 matrix

Plain Text: pay mor eme ney

[PT ends with 2 letters, add 'n' as filler letter]

Cipher Text: pnl mwb (kas) pdh

(Largest set of PT)

-PART A-

Encryption :- Pay

$$(c_1 c_2 c_3) = (P_1 P_2 P_3) \begin{bmatrix} k_{11} & (k_{12}) & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \text{ mod } 26$$

$$(c_1 c_2 c_3) = \begin{pmatrix} p \\ 15 \\ 0 \end{pmatrix} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{ mod } 26$$

$$= 15 \times 17 + 0 \times 21 + 24 \times 2 \quad 15 \times 17 + 0 \times 18 + 24 \times 2 \quad 15 \times 5 + 0 \times 21 + 24 \times 19$$

$$= \begin{pmatrix} 303 \\ 303 \\ 531 \end{pmatrix} \text{ mod } 26$$

$$\equiv (17 \ 17 \ 11)$$

$$\text{mon} = \begin{pmatrix} p_1 & p_2 & p_3 \end{pmatrix} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{ mod } 26$$

$$= \begin{pmatrix} 12 \times 17 + 14 \times 21 + 17 \times 2 \\ 12 \times 17 + 14 \times 18 + 17 \times 2 \\ 12 \times 5 + 14 \times 21 + 17 \times 19 \end{pmatrix}$$

$$\equiv (532 \ 490 \ 677) \text{ mod } 26$$

$$\equiv (12 \ 22 \ 1).$$

$\equiv (m \ w \ b)$ (To be continued)

Decryption:- $p = c \times k^{-1} \pmod{26}$

$$P \quad K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

$$\text{Formula: } K^{-1} = \frac{1}{\det K} \times \text{Adj } K$$

$$\det \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \pmod{26}$$

$$= \{17(18 \times 19 - 21 \times 2) - 17(21 \times 19 - 2 \times 21) + 5(21 \times 2 - 2 \times 18)\} \pmod{26}$$

$$= (5100 - 6069 + 30) \pmod{26}$$

$$= -939 \pmod{26}$$

$$= -3$$

$$= -3 + 26 = 23$$

$\Rightarrow \text{Adj } K =$

$$\begin{array}{|ccc|ccc|} \hline & 17 & 17 & 5 & 17 & 17 \\ \hline 21 & 18 & 21 & 21 & 21 & 18 \\ 2 & 2 & 19 & 2 & 2 & 2 \\ \hline 17 & 17 & 5 & 17 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 & 21 \\ \hline \end{array}$$

$$\text{Adj } K = 18 \times 19 - 2 \times 21 \quad 2 \times 5 - 17 \times 19 \quad 17 \times 21 - 18 \times 5$$

$$21 \times 2 - 19 \times 21 \quad 19 \times \cancel{17} - 5 \times 2 \quad 5 \times 21 - 21 \times 17 \pmod{26}$$

$$21 \times 2 - 2 \times 18 \quad 2 \times 17 - 17 \times 2 \quad 17 \times 18 - 21 \times 17$$

$$= \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{bmatrix}$$

$$\left\{ \begin{array}{l} ((20 \times 2 + 5) \times 25) \mod 26 + (17 \times 12) \mod 26 + (8 \times 18 + 11 \times 81) \mod 26 \\ = 2 \times (14) \times 25 \mod 26 + (17 \times 12) \mod 26 + (8 \times 18 + 11 \times 81) \mod 26 \\ \text{as base } 7 \times 1 \times 8 \mod 26 \end{array} \right.$$

$$\text{so, } k^{-1} = \frac{1}{23} \times \begin{bmatrix} 14 & 25 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{bmatrix} \mod 26$$

$$= 17 \times \begin{bmatrix} 14 & 25 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{bmatrix} \quad \left[\because 23^{-1} \mod 26 = 17 \right]$$

$$= \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 186 \\ 102 & 0 & 17 \end{bmatrix} \mod 26$$

$$\therefore k^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$$17 \times 18 + 17 \times 6 + 17 \times 17 = 17(18 + 6 + 17) = 17 \times 31 = 523$$

$$17 \times 12 + 17 \times 7 + 17 \times 1 + 17 \times 8 + 17 \times 5 = 17(12 + 7 + 1 + 8 + 5) = 17 \times 31 = 523$$

So, the plainText Pay more money

CipherText:- RRL mWBK ASPDH

Solution:-

$$P = C \cdot k^{-1} \pmod{26}$$

$$(c_1 c_2 c_3) = (R R L) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 8 \\ 24 & 0 & 17 \end{pmatrix} \pmod{26}$$
$$= (17 17 14) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \pmod{26}$$

$$= (587 \ 642 \ 544) \pmod{26}$$

$$= (15 \ 0 \ 24)$$

$$= (P \ a \ y) \quad |x| \quad |x| \quad |x|$$

(To be continued)

5

Rail Fence Cipher

- Depth will be given
- Based on depth the sequence will have to be written.

Depth:- 3

Plain Text:- I read Cryptography

I			d		P		r		y
J	a	e	C	y	t	g	a	h	
E					O			P	

Cipher Text:- Iedpruyrdacytgaherop

Decryption:-

x		x				
x	x	x				
x			x			

[x first Blueprint row 2nd then row 3rd]

Gross Value 272

I		d		
J	a			
E	e			

Rail-column Transposition Technique:-

- Sender & receiver is fixed
- Write:- Row by Row
- Read:- Column by Column
- key:- Order of the Column [4 3 1 2 5 6 7]

Example:- Key, - 4 3 1 2 5 6 7

message:- Kill corona virus at twelve am tomorrow

4	3	1	2	5	6	7
K	i	l	l	c	o	r
o	n	a	v	i	r	u
s	a	t	t	w	e	l
v	e	a	m	t	o	m
o	r	p	o	w	y	2

→ Troyas letter to fill empty

Cipher Text:- latwzlv tmo in aer losvo clwtw
oreoy n ulmz

Encryption-2
Decryption-

4	3	1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1020	1021	1022	1023	1024	1025	1026	1027	1028	1029	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1030	1031	1032	1033	1034	1035	1036	1037	1038	1039	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1040	1041	1042	1043	1044	1045	1046	1047	1048	1049	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1050	1051	1052	1053	1054	1055	1056	1057	1058	1059	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1060	1061	1062	1063	1064	1065	1066	1067	1068	1069	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1070	1071	1072	1073	1074	1075	1076	1077	1078	1079	1080	1081	1082	1083	1084	1085	1086	1087	1088	1089	108

Key :- Deceptive

PlainText :- we were discovered

Key :-	D	e	c	e	p	t	i	n	v	e	d	e	c	e	p	t
	3	4	2	4	15	19	8	21	4	3	4	2	4	15	10	

Plain
Text

w	e	a	s	t	e	d	i	v	8	g	q	v	e	s	t	e	d
(22)	4	0	17	4	3	8	18	20	14	21	4	17	4	17	4	3	

Cipher
Text

25	8	2	21	19	22	16	39	6	17	25	6	21	19	22		
2	1	c	v	t	w	g	r	g	r	2	9	v	t	w		

$$3+22=25 \bmod 26$$

$$= 25$$

$$4+4=8 \bmod 26$$

$$= 8$$

Decrypting:- $P_i = (C_i - k_i) \text{ mod } 26$

তাপ্তি value থেকে হুলো করানো Decrypt value

প্রয়োজন সম্ভাৱ।

Cryptography

Eg Crypt means \rightarrow Hidden

graphy means \rightarrow writing

\rightarrow Securing info, data to communication.

\rightarrow Sender will send without any problem. And receiver will receive without any problem.

Feature:

\rightarrow Confidentiality

\rightarrow Integrity :- Info can't be modified.

\rightarrow Non-repudiation :- Can't deny to send Info.

\rightarrow Authentication :- The identities of sender & receiver.

Cyber security:-

The technique of protecting internet connected systems.

Cyber → Systems, networks, programs. & data

Security → protection of all these.

Cyber security goals:-

CIA Triad

Confidentiality: equivalent to privacy

Integrity: Data is authentic, no modification.

Availability: Available, of information

Attacks

Passive: Unauthorized Access

Active: Changing the information.

Cyber Threats Types

→ Malware

→ Phising

→ Man in the middle

→ DDos

→ Brute Force

→ SQL Injection

→ DNS attack

~~Security~~ ~~Security~~

~~Security~~

OSI security

- ↳ Security Attack → Compromises the security
- ↳ Security mechanism → protecting a system
- ↳ Security service

① Security Attacks

(a) Passive Attack

(i) Eavesdropping (Intercept & listen without consent)

(ii) Traffic Analysis (Analyze network to gather info).

(b) Active Attack

(i) Masquerade (Attacker pretends as authentic sender)

(ii) Replay (Intercept a transmitted message & delays or replays it)

(iii) Modification of message

(iv) Denial Of Service:- Attacker sends large volume of traffic.

More of Denial of Service (DoS) Malfunctioning from network or in network situations like

AUT-22

passive vs Active

Passive

Active

- ① Hard to Detect
- ② Neither sender nor receiver is aware of the attack.
- ③ Encryption prevents
- ④ More emphasis

- ① Hard to prevent
- ② Difficult to prevent, physically, software & network vulnerabilities.
- ③ Detect & recover
- ④ Deterrent effect contribute to prevent

2. Security services: - Different services available to maintain the security. 5 types.

- (i) Authentication
- (ii) Access control
- (iii) Data Confidentiality
- (iv) Integrity (Data is not changed)
- (v) Non-repudiation (verifiable record to make sure authentic sender sent message)

Sem-2
2010

3] Security mechanism:

(i) Encryption

(ii) Digital signature

(iii) Traffic padding (Add extra data in network traffic stream)

(iv) Routing protocol (select routes when a gap in security is suspected)

A Model For Network Security

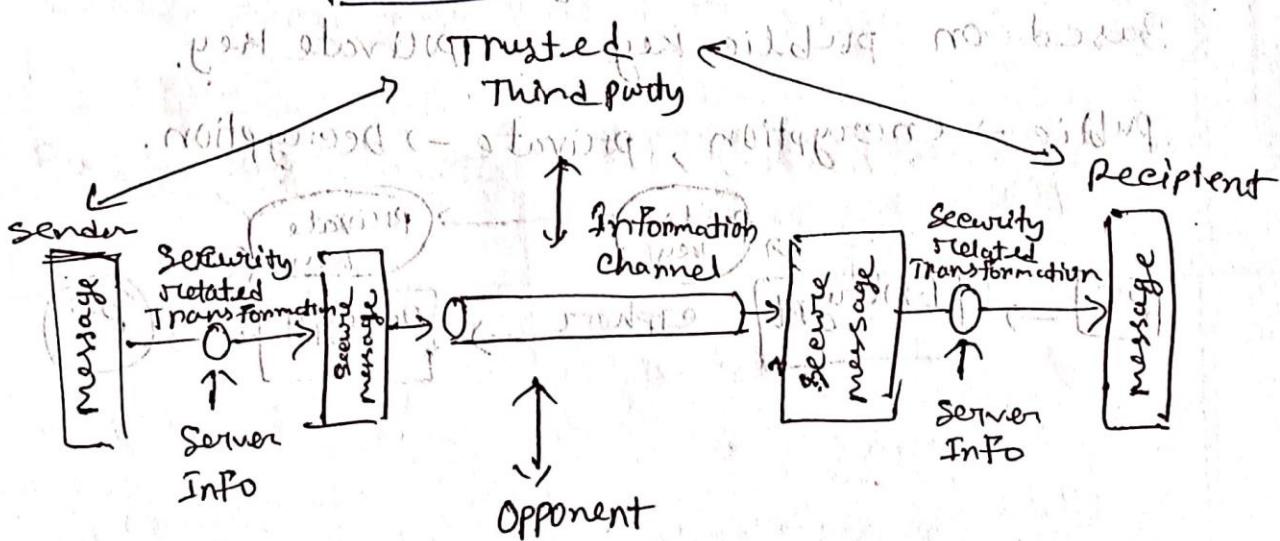
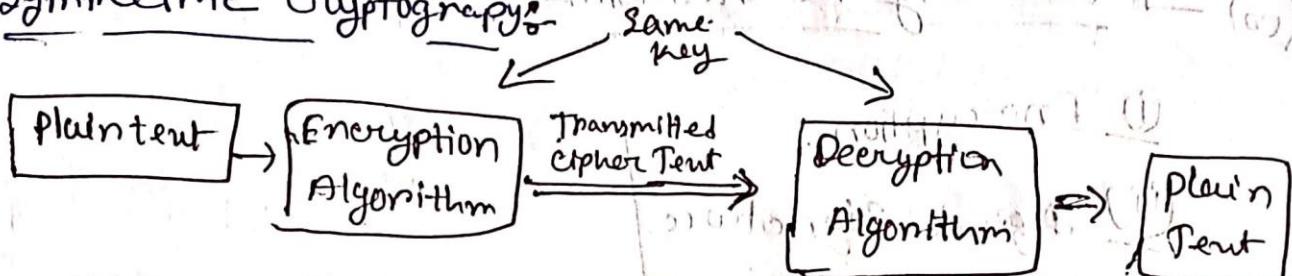


Fig : Model For Network Security.

Aut-22 2(a)

Spring - 2(a)

Symmetric cryptography



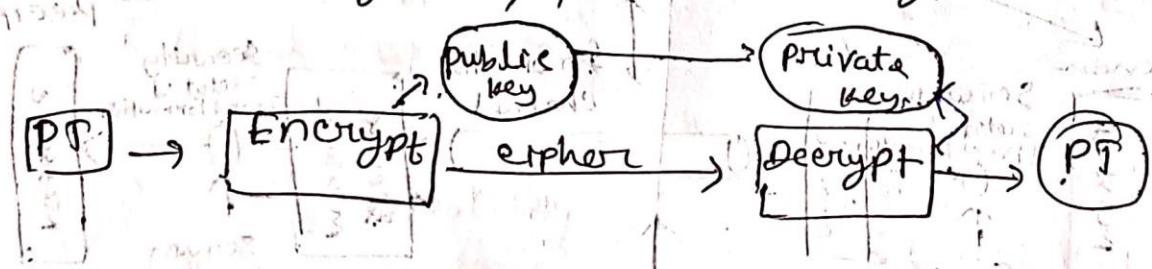
→ Change of any message in order to protect it from reading by anyone. Same key

(b) Asymmetric Cryptography
For Encrypt & ~~key~~ decryption.

Asymmetric cryptography

Based on public key & private key.

public → encryption, private → Decryption.



PT → Encrypt → cipher → Decrypt → PT

Block vs Stream

SP51-20
30/09/2019

Block vs Stream

Block

Stream

- | | |
|---|---|
| <p>① Converts by taking plain text's block at a time.</p> | <p>① Converts by taking 1 byte of plain text</p> |
| <p>② 64 bits or more</p> | <p>② 8 bits</p> |
| <p>③ Complexity \rightarrow simple</p> | <p>③ Complexity \rightarrow more</p> |
| <p>④ Confusion & deFusion</p> | <p>④ Only Confusion</p> |
| <p>⑤ Reverse encrypted text is hard.</p> | <p>⑤ Easy.</p> |
| <p>⑥ Fixed-length blocks</p> | <p>⑥ bit or byte at a time.</p> |

Cryptography

FINAL

AES [Advanced Encryption Standard]

=> Encryption algorithm. worldwide use ~~2013~~ 2014

(about) Symmetric Key Block Cipher :-

Some keys are used for encryption + decryption.

Fixed - block size = 128 bits

[16 bytes = 4 words] 1 word
= 32 bits
4 bytes

Rounds	No. of bits in key
10	128
12	192
14	256

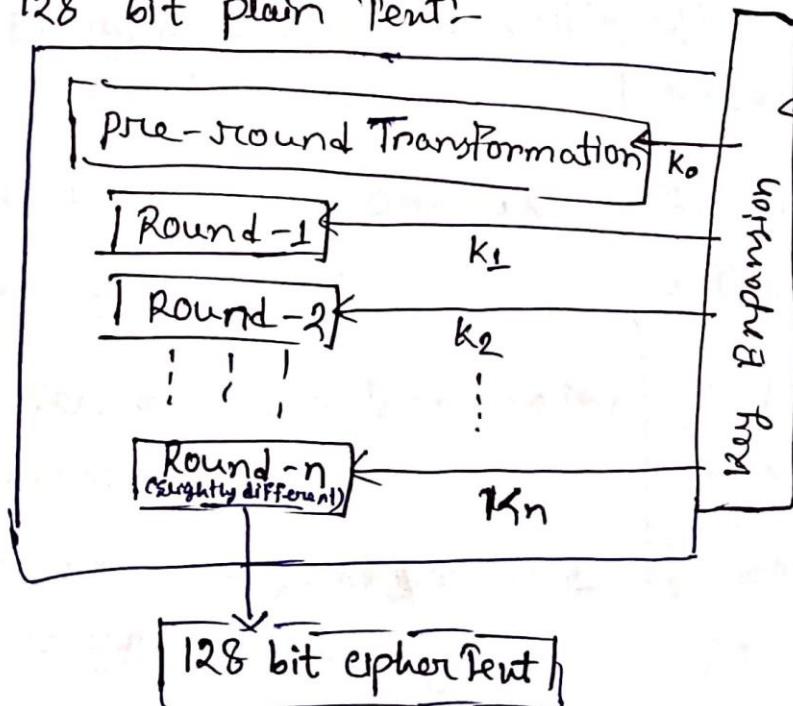
AES-128 version

AES-192 version

AES-256 version

General Design of AES

128 bit plain Text:-



Cipher key
[128, 192 or 256 bit]

Fig:-
General design
of
AES Encryption

1 byte = 8 bits

1 word = 4 bytes

= $4 \times 8 = 32$ bits

Block size = 128 bits

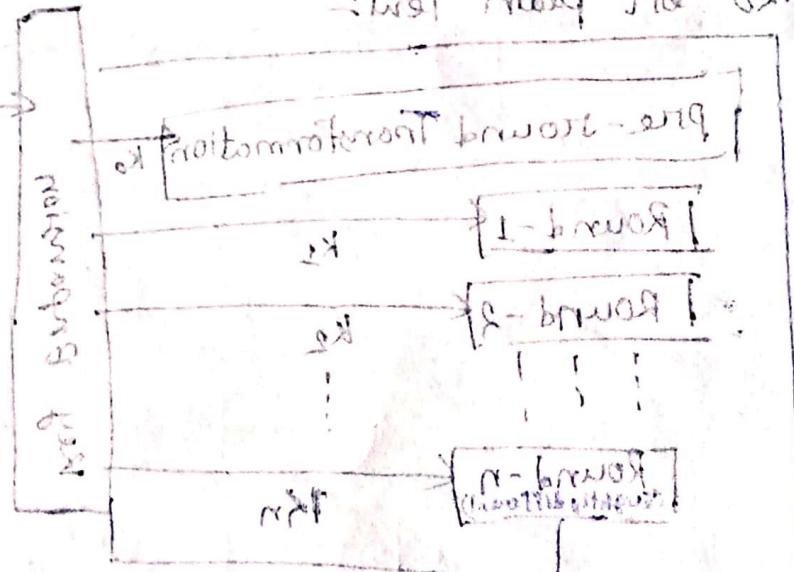
No. of keys generated by key expansion = $(\text{No. of rounds} + 1)$

16 bytes (4×4) matrices

Input Array - ($4 \times 4 = 16$ bytes, 128 bits or 4 words)

$S_{0,0}$	$S_{0,1}$													
$S_{1,0}$	$S_{1,1}$													
$S_{2,0}$	$S_{2,1}$													

note word = 4 bytes
row or column = 4 bytes



$$\text{Col } 0 = \text{word 1}$$

$$\text{Col } 1 = \text{word 2}$$

$$\text{Col } 2 = \text{word 3}$$

$$\text{Col } 3 = \text{word 4}$$

Steganography:-

The practice of concealing information within or physical objects to avoid detection.

105/10
प्रश्न ५

concealing information within or physical objects to

The difference between cryptography & Steganography:

cryptography	Steganography
① Secure Content message	① Hide the existence message.
② Hidden message is not apparent	② Encrypted message visibly scrambled.
③ Ciphertext is obvious but unreadable	③ Difficult to detect without specific tools.
④ Secure data transmission, authentication etc.	④ Digital object management.
⑤ Symmetric, asymmetric encryption, hashing, digital signature.	⑤ Embedding data in LSB

⑥ Hiding

⑥ Can be combined with
of stenography, etc.

Information hiding [6]

⑥ Can be combined
with cryptography

Cryptography

Encryption and decryption
of messages

③

test of appearance rabbit
(fork) - trachea

test of the lifting
about 50 days

appearance before lifting
trees

at about 50 days

83

Cryptography

protect the data message [1]

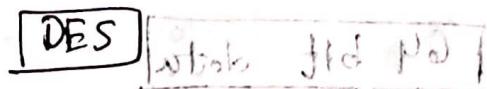
③
of messages - rabbit
trachea - fork

③
cyclic sequence algorithm
of messages

③
around of trachea
about 50 days

③
cyclic sequence algorithm
of messages

③
disturbances, disturbances
faint sound, etc., messages
waterproof, waterproof



→ 64 bit plaintext block.

↳ 16 rounds, each round is a Feistel round.

Steps:-

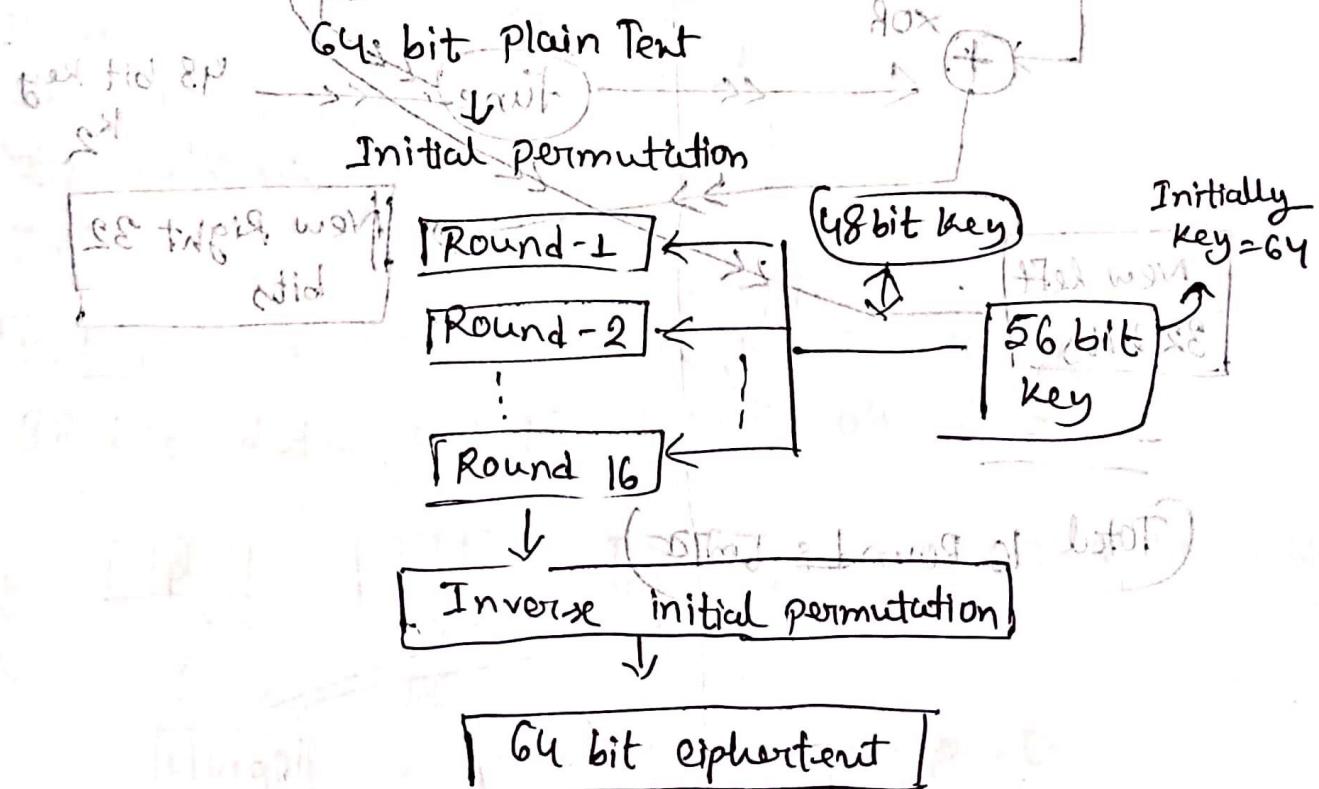
(1) Initial permutation.

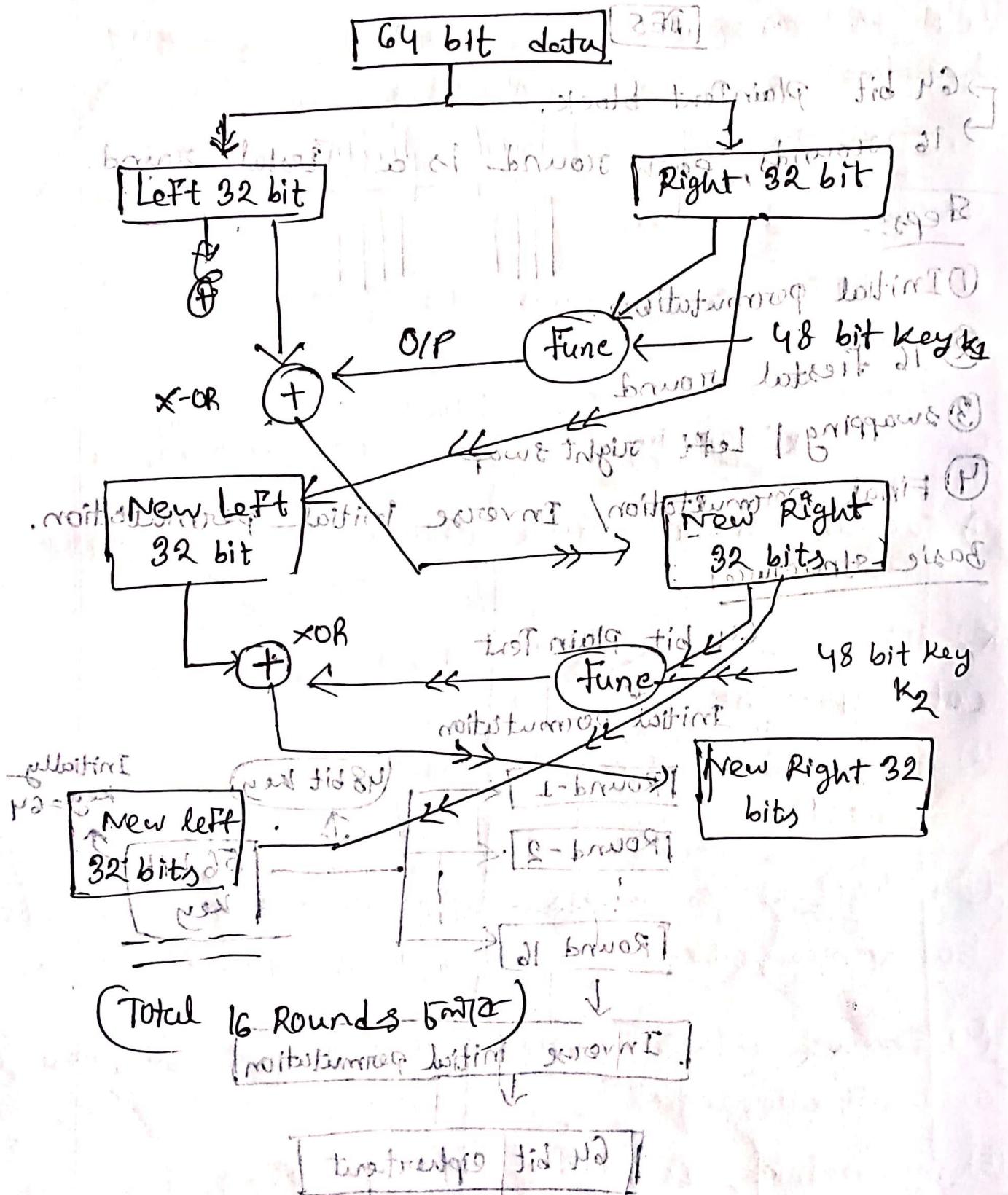
(2) 16 Feistel round

(3) swapping | Left right swap

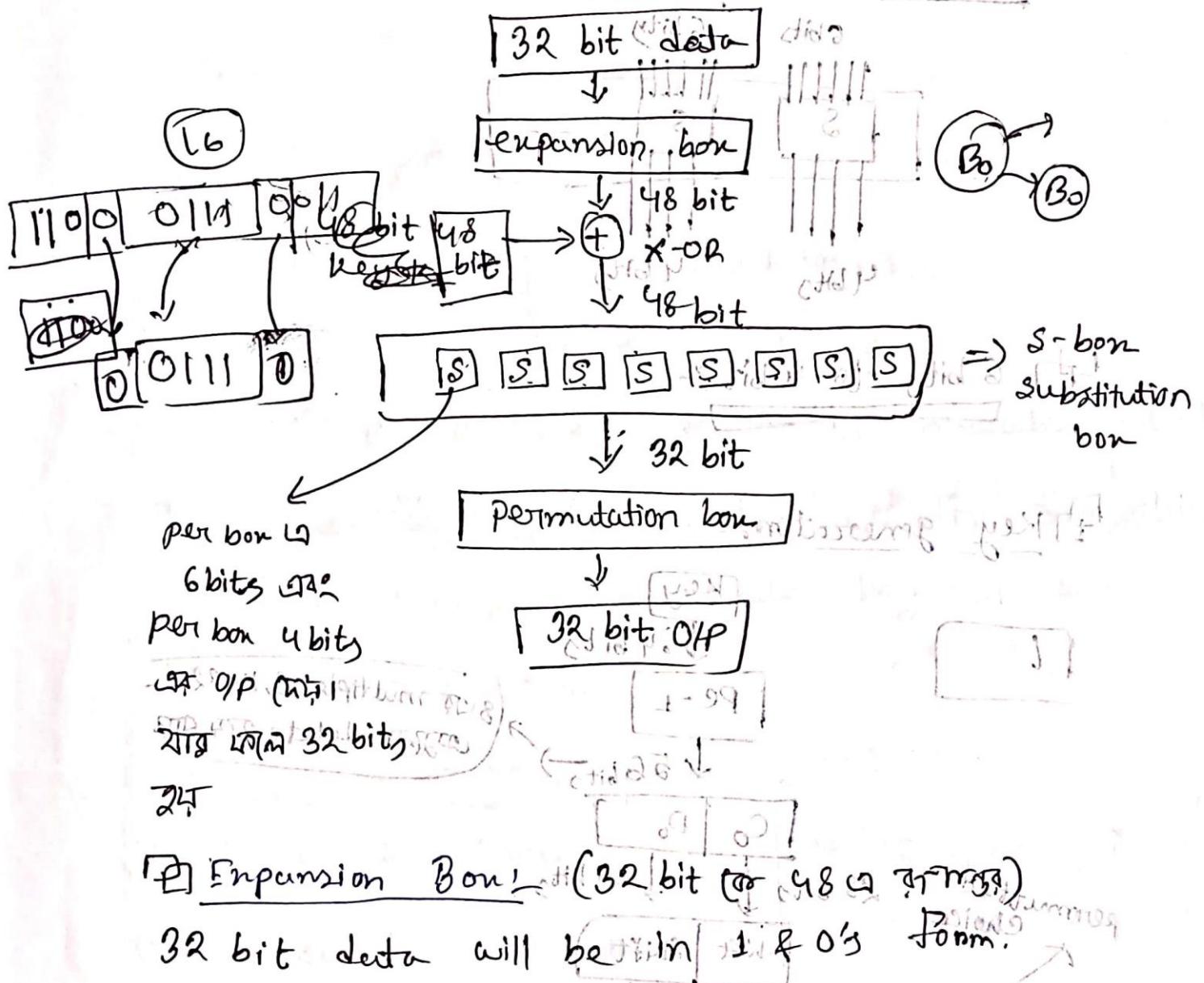
(4) Final permutation/ Inverse initial permutation.

Basic structure:-



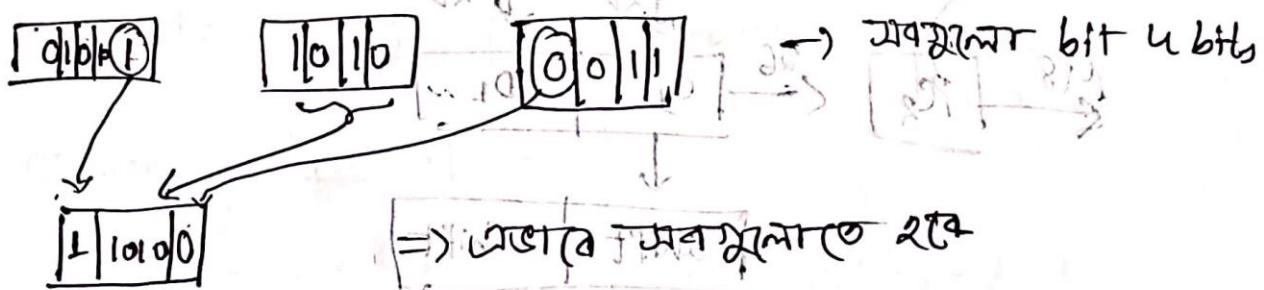


Func. (function definition) : if id (p) = mod - 2 由

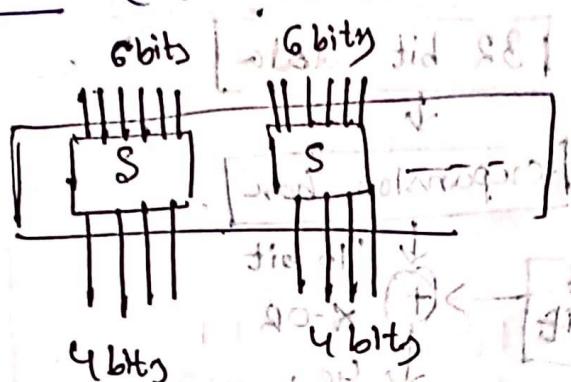


Expansion Bound (32 bit or 48 bit strings)

32 bit data will be in 1's & 0's form.



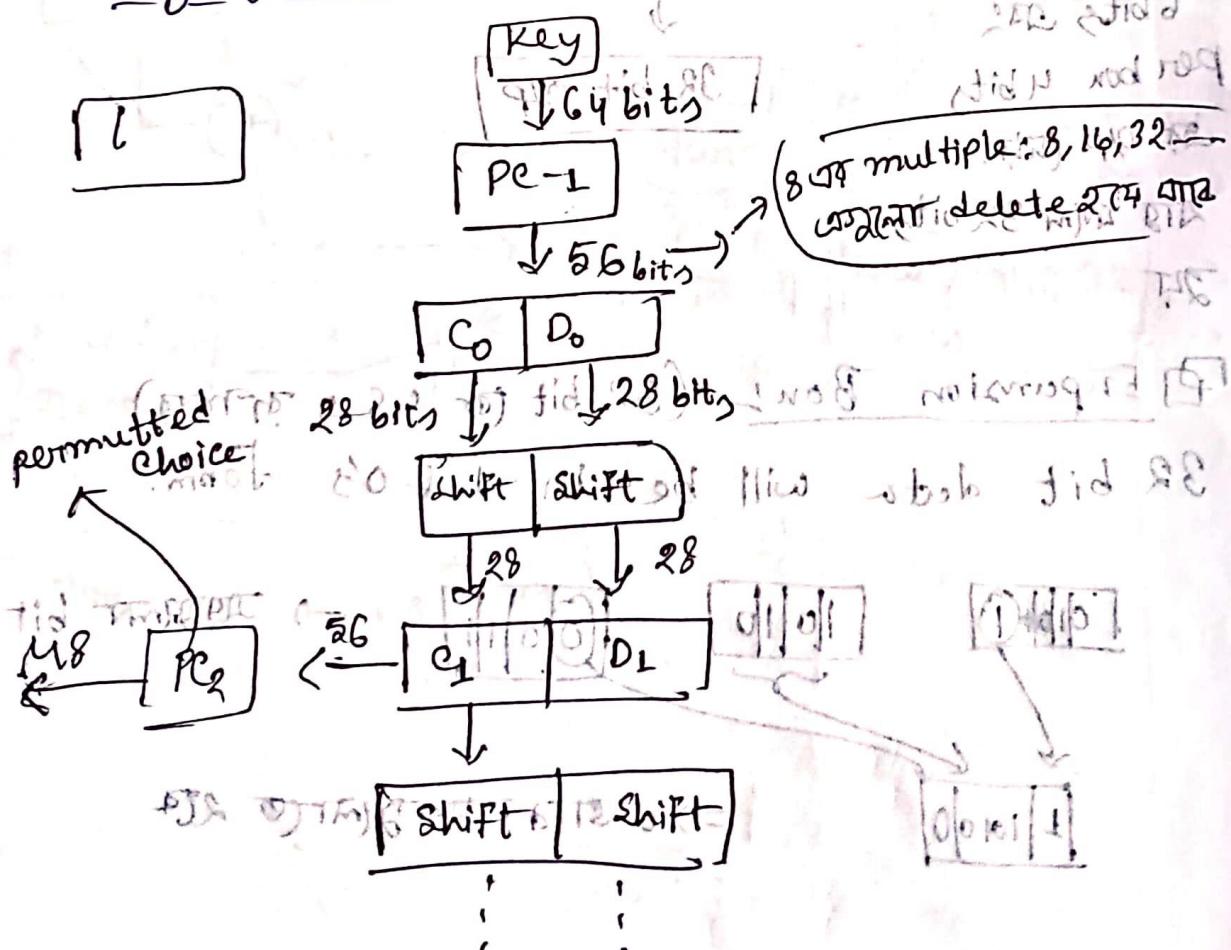
S-box :- (48 bits \rightarrow 32 bits) (G2 convert)



6 bits to 4 bits :-



Key generator:



111000

(101)

$\boxed{\square}$ RSA Algorithm :- Rivest-Shamir-Adleman

An asymmetric Cryptographic algorithm.

• Public key → Known to all users in n/w

Private key → Kept secret, (not) shareable at all.

If = (Public Key) of user-A is used for encryption,
we have to use the private key of same
user for decryption.

1] Key Generation:-

(1) Select 2 large prime. $P & Q$

(2) Calculate ; $n = P * Q$

(3) Calculate $\phi(n) = (P-1) * (Q-1)$ [Euler Totient]
 $E = b, D = g^{-1} \pmod{n}$

(4) choose value of e

$1 < e < \phi(n)$ & $\gcd(\phi(n), e) = 1$

(5) calculate $d = e^{-1} \pmod{\phi(n)}$

$$cd \equiv 1 \pmod{\phi(n)}$$

(6) public key = {e, n}

(7) private key = {d, n}

Question

$$P=3$$

, $Q=11$ since $\phi=7$ from $\phi(n)=\phi(p-1)(q-1)$

$$n = P \cdot Q = 3 \cdot 11 = 33$$

$$\text{Also } \phi(n) = (P-1) \cdot (Q-1) = 2 \cdot 10 = 20$$

so, let $e=7$ as $1 < e < 20$ & $\gcd(7, 20) = 1$

now, for finding d we have to find d such that

$$d = e^{-1} \pmod{\phi(n)}$$

$$7d = 1 \pmod{\phi(n)}$$

$$\frac{d}{7} \cdot \text{mod } \phi(n) = 1 \pmod{\phi(n)} \quad \text{using step 3 to 2}$$

$$\frac{d}{7} \cdot 7 \cdot d = 1 \pmod{\phi(n)} \quad \text{as } 7 \cdot d = 1 \pmod{\phi(n)} \quad (3)$$

$$(7 \cdot d) \pmod{20} = 1 \quad (\because d = 3)$$

$$(1 \cdot 3)^2 \pmod{20} = 1^2 \pmod{20} = 1 \pmod{20} \quad (4)$$

$$\text{Since, } e=7, d=3$$

$$\text{Public key} = \{e, n\} = \{7, 33\} \quad (5)$$

$$1 = (2, (n)^p) \text{ form } (n)^p > 2 > 1$$

$$\text{private key} = \{d, n\} = \{3, 33\} \quad (6)$$

$$(n)^p \cdot \text{form } 1 = b$$

Encryption (RSA)

$$C = M^e \text{ mod } n \quad [m = 31] \quad M \in \mathbb{N}$$

$$C = 31^7 \text{ mod } 33 \quad [e, n \text{ public key used in Encryption}]$$

Decryption

$$M = C^d \text{ mod } n \quad [d, n \text{ private key used in decryption.}]$$

$$= 4^3 \text{ mod } 33 = 31$$

Euler's Totient Function

\Rightarrow represented using phi as $\varphi(n)$ & may also be called Euler's phi function.

$\varphi(n)$ is defined as the number of integers,

$$\varphi(5) = \{1, 2, 3, 4\} = 4 \quad [\text{values that are } \text{gcd } 1 \text{ with } 5] \quad [\text{Euler's Totient}]$$

$$\varphi(6) = \{1, 5\} = 2$$

When n is prime, $\varphi(n) = n - 1$

$$\varphi(5) = 4$$

$$\varphi(25) = 24$$

$\Phi(n) = \phi(a+b) = \phi(a) * \phi(b)$ [$a & b$ should be coprime]
 $n \leq m$ [$1 \leq n \leq m$] n both $\text{gcd} = 1$

$$\Phi(15) = \Phi(3) * \Phi(5) = 2 * 4 = 8$$

[integers less than n , $\neq 0$] $P =$
 Diffie Hellman

→ NOT encryption algo

private key exchange b b b
 → used to exchange key between sender & receiver.

④ Algorithm

① Consider prime number p

② Select a such that it must be the primitive root of p

primitive root of p & $a \neq 1$

(primitive root check -)

$$at \text{ mod } p : \{ 1, 2, \dots, p-1 \} = (\mathbb{Z}/p\mathbb{Z})^*$$

$$a^2 \text{ mod } p = \{ 1, 2, \dots, p-1 \} = (\mathbb{Z}/p\mathbb{Z})^*$$

$$a^3 \text{ mod } p = \{ 1, 2, \dots, p-1 \} = (\mathbb{Z}/p\mathbb{Z})^*$$

$$1-a = (\mathbb{Z}/p\mathbb{Z})^*$$

$$p = (\mathbb{Z}/p\mathbb{Z})^*$$

$$p = (\mathbb{Z}/p\mathbb{Z})^*$$

$$\text{For mod} \equiv (A-A) \div (B \times B)$$

Alice, Bob \Rightarrow prime, $q=17 \rightarrow (n)$

$$[x^2 = 5]$$

$$\sqrt{x} = 5 \rightarrow (a)$$

Alice, Secret, $s_a = 4$ (sender)

$$[x^2 = 6]$$

Bob n , $s_b = 6$ (receiver)

So, public key,

$$\text{Alice, } y_a = (a)^{s_a} \mod n \text{ where } n = 17$$

$$= (5)^4 \mod 17$$

$$= 13$$

$$\text{Bob, } y_b = (a)^{s_b} \mod n$$

$$= (5)^6 \mod 17$$

$$= 16$$

NOW, Secret key,

$$\text{Alice, secret key} = (y_b)^{s_a} \mod n$$

$$= (16)^4 \mod 17$$

$$= 16$$

$$\text{Bob, secret key} = (y_a)^{s_b} \mod n$$

$$= (13)^6 \mod 17 = 16$$

RSA algorithm - ⑤ algorithm &

$$\text{encryption} = (C \equiv P^e \pmod{n}) \rightarrow \begin{matrix} \text{Public key} \\ \downarrow \quad \downarrow \\ \text{cipher plain} \end{matrix}$$

$$\text{Decryption: } P = C^d \pmod{n} \rightarrow \begin{matrix} \text{Private key} \\ \text{public key} \end{matrix}$$

$$\text{public key} = \{e, n\}$$

$$\text{private key} = \{d, n\}$$

$$81 \text{ base } 88 = 81 \text{ base } 18$$

$$81 \text{ base } 18 = 81 \text{ base } 88$$

$$81 \text{ base } 281 = 81 \text{ base } 88$$

math-

$$P = 17, q = 11, - e = 7, M = 88 \quad (17 \times 11 \times 88) =$$

$$n = 17 \times 11 = 187$$

$$\varphi(n) = (17-1) \times (11-1) = 160$$

we know,

$$d = e^{-1} \pmod{\varphi(n)}$$

$$\Rightarrow d \cdot e \pmod{\varphi(n)} = 1$$

$$\Rightarrow d \cdot 7 \pmod{160} = 1$$

$$\Rightarrow 23 \cdot 7 \pmod{160} = 1$$

$$d = 23$$

$$M = 81 \text{ base } 88$$

$$M = 81 \text{ base } (17 \times 11 \times 88)$$

∴ Encryption, $C = M^e \text{ mod } (n)$

$$= (88)^7 \text{ mod } (187)$$

$$\begin{array}{r} 64826842 \\ \times 11 \\ \hline 0111 \end{array}$$

$$\begin{array}{r} 64826842 \\ \times 10000 \\ \hline 0111 \end{array}$$

$$88^1 \text{ mod } 187 = 88 \text{ mod } 187$$

$$77^2 \text{ mod } 187 = 77 \text{ mod } 187$$

$$\leftarrow (88^4 \text{ mod } 187 = 132) \quad 77^2 = 132 \text{ mod } 187$$

$$= (88 \times 77 \times 132) = 894432 = 11 \text{ mod } 187$$

$$= 11$$

$$\therefore C = 11.$$

2. Decryption $\Leftarrow C^d \text{ mod } (n)$

$$= (11)^{22} \text{ mod } 187$$

$$(8421 \text{ mod } 187)^{22}$$

$$11^1 \text{ mod } 187 = 11$$

$$11^2 \text{ mod } 187 = 121$$

$$11^4 \text{ mod } 187 = 55$$

$$11^8 \text{ mod } 187 = 71$$

$$21435881$$

$$(11 \times 121 \times 71) \text{ mod } 187 = 88$$

(3b) Euler's Totient: How to find?

Euler's Function $\phi(n)$, counts the number of positive no. relatively prime to n .
Integers up to n that are relatively prime to n .

Example:-

$$n = 9$$

numbers less than 9 are 1, 2, 3, ~~4, 5, 6, 7, 8~~
so, the integers less than 9 are 1, 2, 3, ~~4, 5, 6, 7, 8~~

The numbers that are coprime with 1, 2, 4, 5, ~~6, 7, 8~~

∴ Therefore, $\phi(9) = 6$

General formula:-

$$\text{If } n = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} \text{ then } \phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$$

example:- $n = 12$

prime factorization $= 2^2 \times 3$

$$\phi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right)$$

$$= 12 \times \frac{1}{2} \times \frac{2}{3} = 4$$

(Subtract from total numbers) \rightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

∴ Now we want knowledge of

what are these prime numbers

and which are composite numbers

Concept of Network Penetration Testing

A process used to evaluate the security of a computer network by simulating an attack.

Key Concepts:-

(1) Gathering info about target network to identify potential entry points.

- (2) using tools to scan the network.
- (3) Developing custom exploits to breach network defenses.

(4) Once access is gained, the focus shift to maintaining access, gathering info.

(5) Documenting findings, providing detailed reports to stakeholders.

Penetration Testing

- (1) planning:
 - Define scope & goal
 - Collect (domain names, mail servers etc) to understand how target works.

- (2) Scanning:
 - Inspect the code
 - Inspect the application

(3) Granting of access ~~Granting of access~~ & new teams
↳ Involves setting up of roles & privileges

(4) Maintain Access

(5) Analysis & Reporting

(6) Clean-up

Network penetration testing is a critical component of an organization's cybersecurity strategy. It involves a systematic approach to identifying, exploiting & documenting vulnerabilities within a network to improve its security defenses.

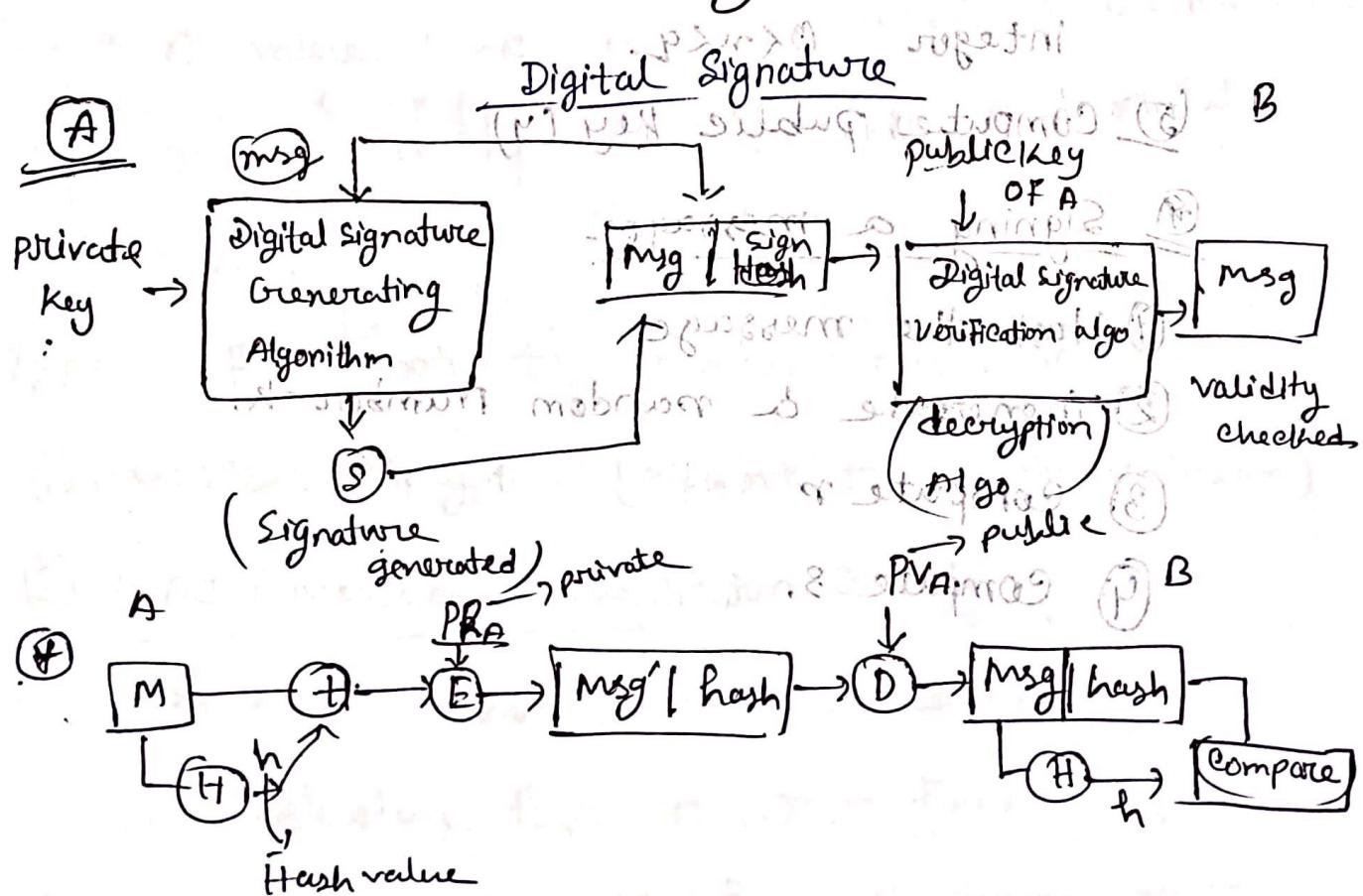


Fig 1- Concept of D.Signature

- Must use same info unique to the sender to prevent the denial.
- It must be easy to produce digital signature.
- Easy to verify & recognize signature.

④ Key generation

- ① choose a prime number P_1
- ② choose a prime number P_2
- ③ choose g ; $g = P_1 \cdot P_2$
- ④ choose private key (w) - A randomly chosen integer $0 \leq w \leq q$

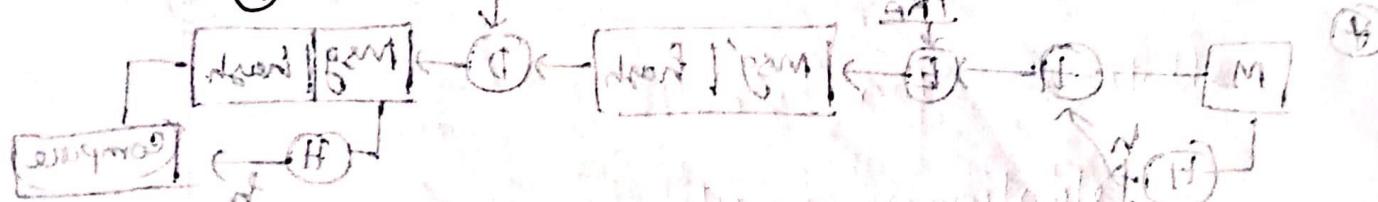
⑤ Compute public key (y)

⑥ Signing a message:-

- ① Hash the message.
- ② Generate a random number k .

- ③ Compute r

- ④ Compute s .



unauthorized to send a msg

Confidentiality:- Refers to protecting the information from being accessed by unauthorized parties.

Data Integrity:- Data modification.

Authentication:- verify the user's identity.

Authentication Functions

Authenticator must be there to authenticate the message. → A value which is sent used to authenticate message & a function is which authenticate a message.

Types of Function to produce Authentication

① message Encryption (ciphertext) -> (Authenticator)

② MAC (Message Authenticator Code):-

$C(m, k)$ = Fixed length code (Code)(MAC)

any messages fixed or variable length

Convert msg to binary & then authentication Verify

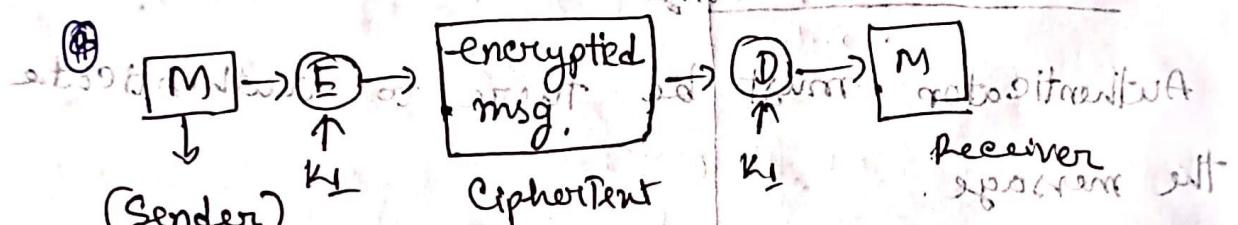
(iii) Hash Function:

msg \rightarrow H(M) = fixed length code (Hash Code 'h')

Independent OF key

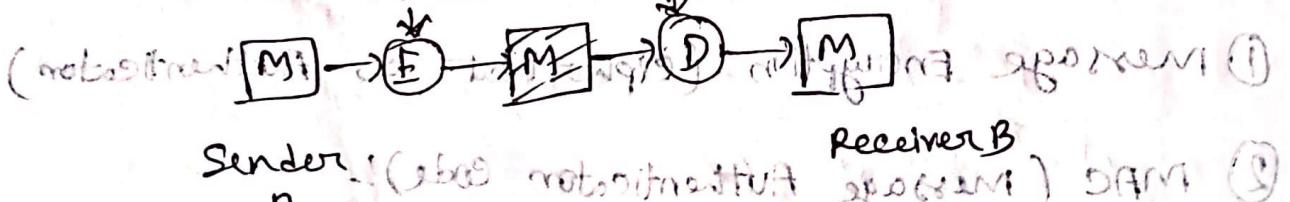
Dynamically changing entity \rightarrow Message Encryption:

⊕ ciphertext is an authenticator.



→ Key K_1 is shared between sender & receiver only. [Both key same = Asymmetric]

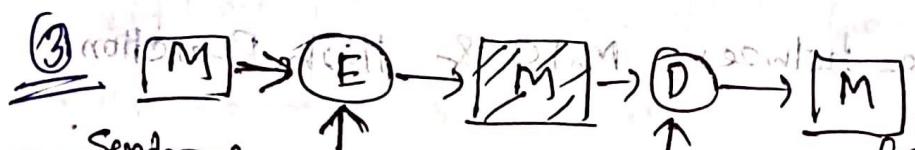
② Symmetric :- [Different key].



→ Here Authentication is not available.

→ But Confidentiality is available.

→ Confidentiality is achieved by frequent



Sender-A

(Receiver-B)

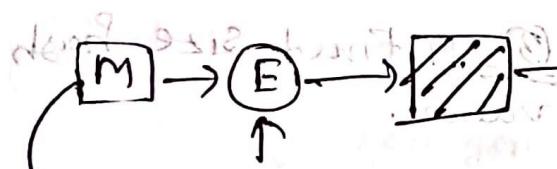
K private A

K public A

Authentication available

Confidentiality not available.

④ To get both



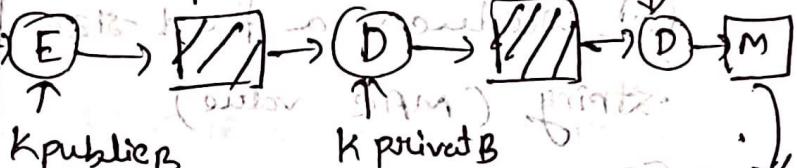
K private A

Alice
sender

Authentication & Confidentiality!

K public A

Cipher



K private B

K public B

not been
intercepted

confidentiality &完整性 not

confidentiality not low

confidentiality source of

confidentiality & integrity

intercepted

confidentiality &完整性 not

target group of intercepting agencies

can review it with tanks news or

any other news

confidentiality &完整性 not

$$(S^H)H = (W)H$$

different words results in framing of cipher with

5)

Difference between MAC & Hash Function

MAC (Message Authentication Code)	Hash Function
① provides data integrity & authenticity.	① provides data integrity only.
② Takes a message & a secret key as input.	② Takes only a message as input.
③ produces a fixed size string (MAC value).	③ A fixed size hash value.
④ Requires a secret key for generation & verification.	④ No key required for generating hash values.
⑤ Used for authentication to ensure message authenticity & integrity.	⑤ Used for data integrity verification

Security of Hash Functions:-

① Preimage Resistance:

→ Computationally infeasible to find any input x , such that $H(x) = h$, where h is a given hash value.

② Second Preimage Resistance:

$$H(u_1) = H(u_2)$$

This helps to prevent an attacker from finding

(for more) SAM

a different message that has the same hash value as the given message.

B) Collision Resistance

Ensures that two different messages can't produce the same hash value.

Security of MAC:

i) Confidentiality of the key

→ Key management practices are critical, including using strong, random keys & protecting them from unauthorized access.

ii) Resistance to Forgery

→ A secure MAC should make it computationally infeasible for an attacker to generate a valid MAC for a message without knowing the secret key.

iii) Replay Attack prevention

An attacker uses a valid message & its MAC deceive the receiver.

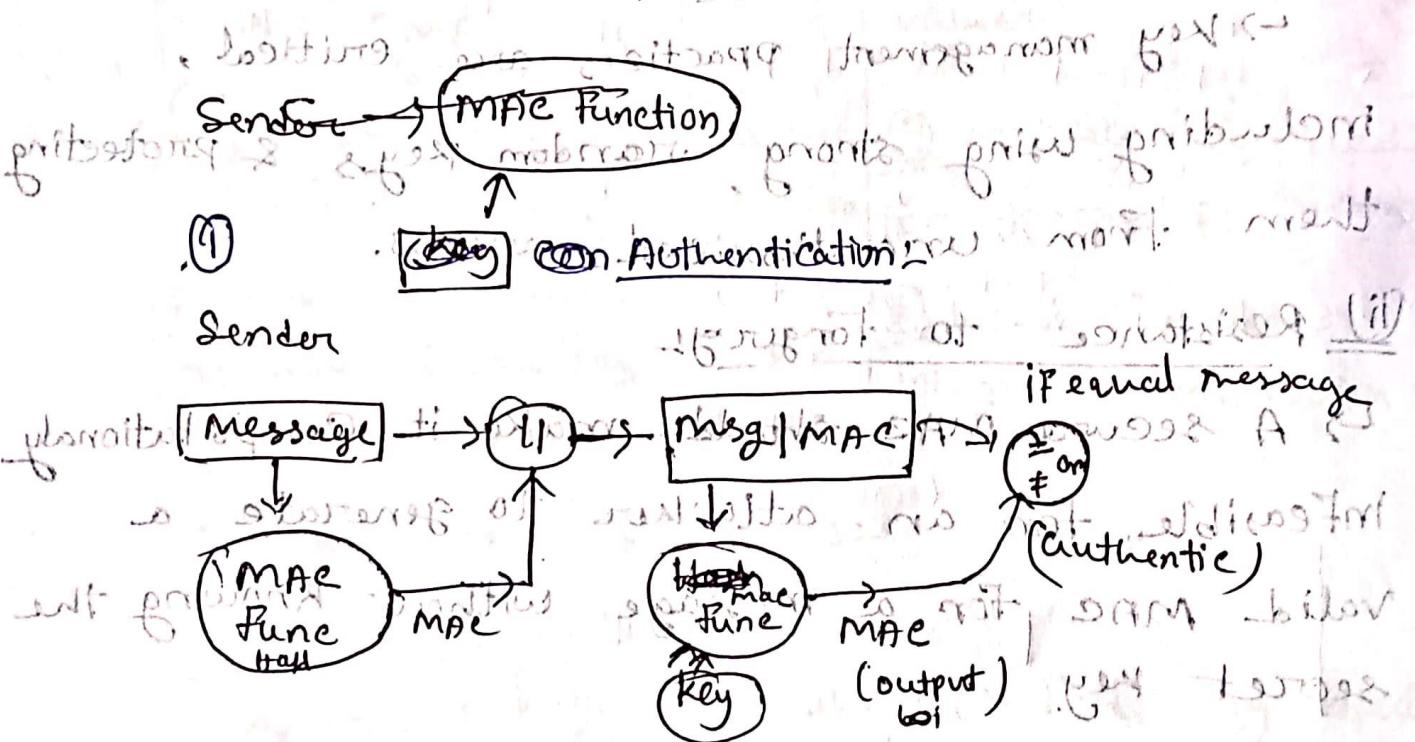
iv) Algorithm Security

The underlying cryptographic algorithm be secure against known attacks.

Signatures form next topic Stream cipher etc.

MAC (From rd)

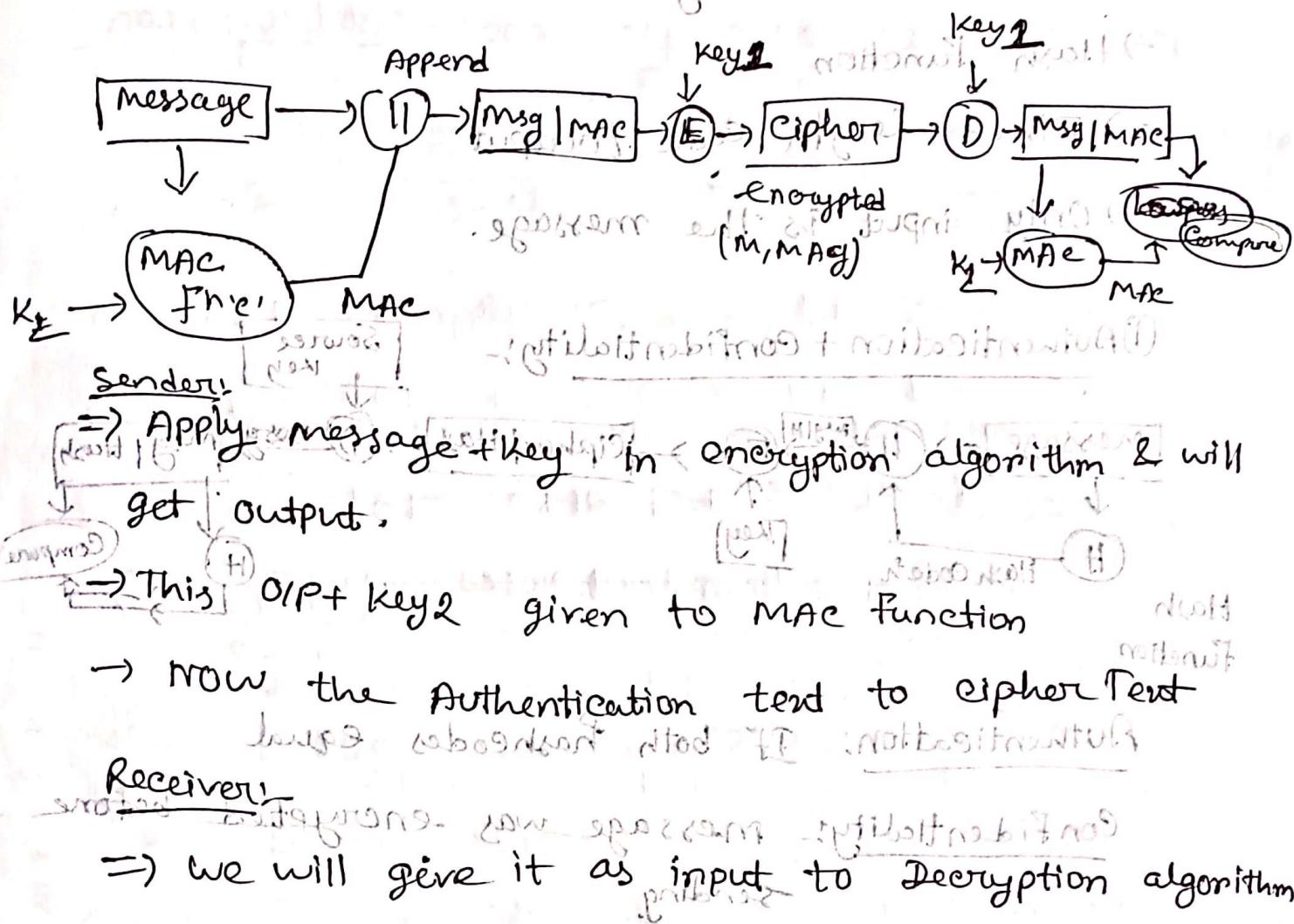
- will use ~~and~~ a secret key for transmission
 - Generate a ~~small~~ fixed size of data called MAC.
 - Then will append with the message.
 - Sender, receiver will have a secret key.
- ① $A \rightarrow B$
- $$MAC = C(K, M)$$
- Key (common) message



Here, Hash Func added to message new receiver can check SAM & if same then message creates. Then again the MAC func is used with key. Again an ~~Mac~~ Output is generated which is MAC. If equal they are authentic if not then not authentic.

(b) multi-key

② Authentication & Confidentiality

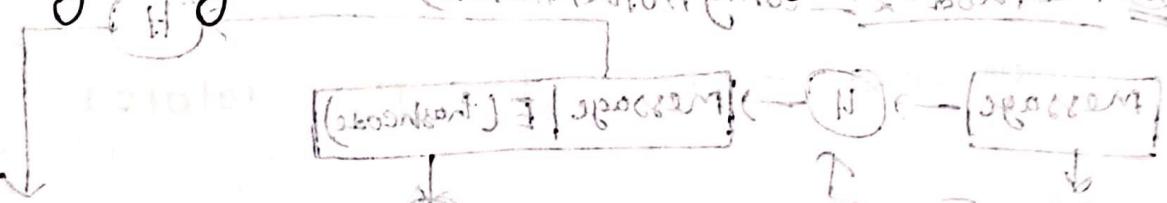


→ Now the Authentication tend to cipher Text

Receivers

⇒ we will give it as input to Decryption algorithm

using key -1 & output message.



we shift processing

TOP layer part ends

Hash from (vd)

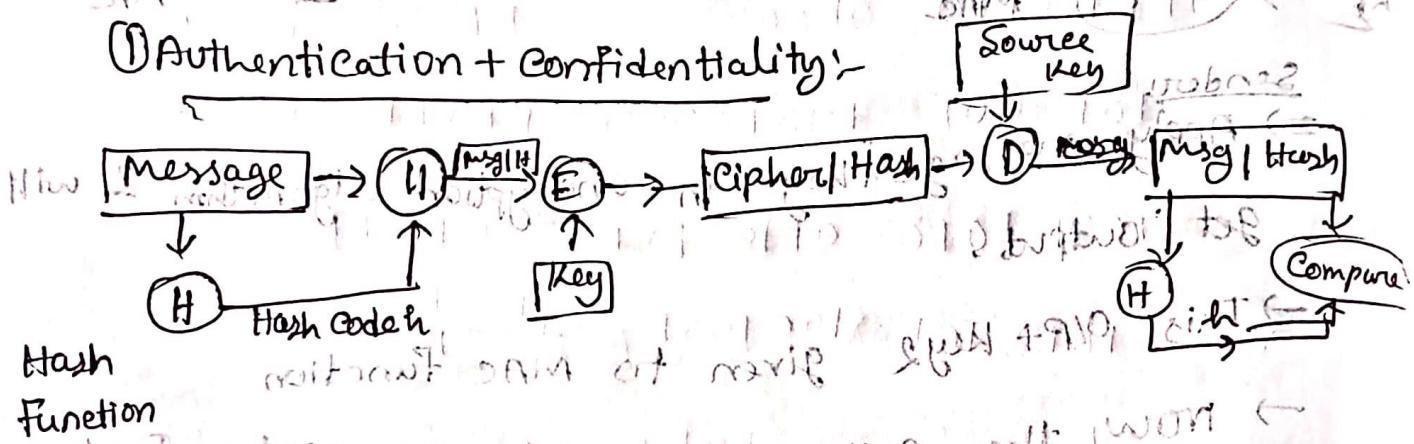
→ Does not use a key like MAC

→ Hash Function

→ Fixed length code / output

→ Only input is the message.

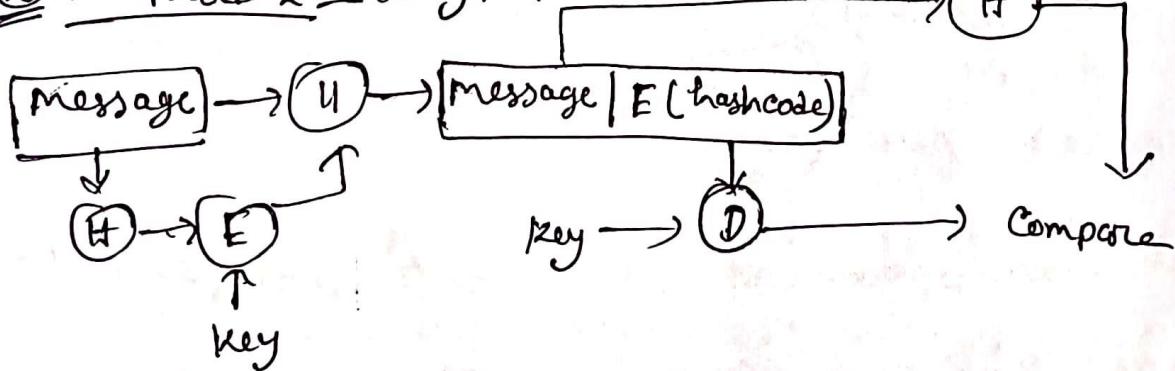
(1) Authentication + Confidentiality:-



Authentication:- If both hash codes equal

Confidentiality:- message was encrypted before sending.

(2) method-2: (Only Authentication)

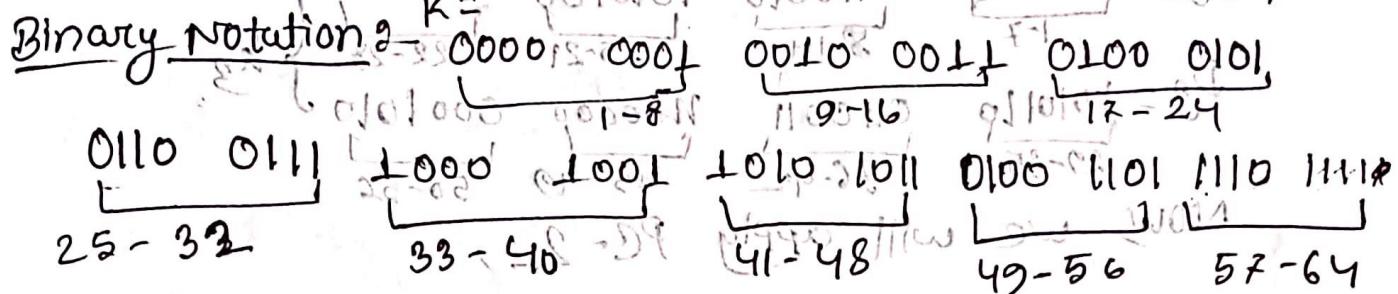


→ processing time low

→ Same key used

DES

Method 3



Now, we will apply 56 bit PC-1.

$$C_0 = \underbrace{00000001}_{1001+8} \quad \underbrace{00100011}_{0110+36} \quad \underbrace{01000101}_{17-24} \quad \underbrace{01000111}_{25-32}$$

$$D_0 = \underbrace{10001001}_{1010+8} \quad \underbrace{10101011}_{1010+36} \quad \underbrace{01001101}_{17-24} \quad \underbrace{11101111}_{25-32}$$

$$K' = \underbrace{10110000}_{01010000} \quad \underbrace{00101010}_{00101010} \quad \underbrace{10100010}_{10100010} = 8^1$$

$$\text{TOTOTOTO TOTOTOTO TOTOTOTO TOTOTOTO}$$

$$\text{TOTOTOTO TOTOTOTO TOTOTOTO TOTOTOTO}$$

$$C_0 = 10110000 \quad 01100111 \quad 00101010 \quad 01000000$$

$$D_0 = 10101010 \quad 01100111 \quad 00111110 \quad 00000000$$

$$C_1 = \underbrace{01100000}_{1-7} \quad \underbrace{11001100}_{8-15} \quad \underbrace{01010100}_{15-21} \quad \underbrace{10000000}_{22-28}$$

$$D_1 = \underbrace{01010100}_{29-35} \quad \underbrace{11001100}_{36-42} \quad \underbrace{01111000}_{43-49} \quad \underbrace{00000000}_{50-56} \quad \left\} k_1 \right.$$

$$C_2 = \underbrace{11000010}_{1-7} \quad \underbrace{10011000}_{8-14} \quad \underbrace{10101010}_{15-21} \quad \underbrace{00000100}_{22-28} \quad \left\} k_2 \right.$$

$$D_2 = \underbrace{10101010}_{29-35} \quad \underbrace{10011000}_{36-42} \quad \underbrace{11110000}_{43-49} \quad \underbrace{00000000}_{50-56} \quad \left\} k_2 \right.$$

Exhortation

$$C_3 = \underline{0000110} \quad \underline{0110010} \quad \underline{1010100} \quad \underline{0001011} \\ 1010 \quad 0010 \quad 1100 \quad 0000 \quad 22-28 \quad k_3$$

$$D_3 = \underline{1010110} \quad \underline{0110011} \quad \underline{1100000} \quad \underline{0001010} \quad 1110 \quad 0110 \\ 1111 \quad 0111 \quad 1011 \quad 0000 \quad 50-56 \quad 22-28$$

NOW, we will apply PC-2, i.e.

$$k_1 = \underline{000000011} \quad \underline{000000010} \quad \underline{01100111}$$

$$10011011 \quad 01001001 \quad 10100101 \\ 1100110 \quad 1010010 \quad 1010010$$

$$k_2 = \underline{01101000} \quad \underline{10100110} \quad \underline{01011001}$$

$$10011011 \quad 01001001 \quad 10100101 \\ 1100110 \quad 1010010 \quad 1010010$$

$$k_3 = \underline{01000101} \quad \underline{11010100} \quad \underline{00000101}$$

$$1000010 \quad 1101010 \quad 0000010 = 4 \\ 10110100 \quad 00101000 \quad 11010010$$

$$0000000 \quad 0111100 \quad 1100110 \quad 1010101$$

∴ k_1, k_2, k_3 are obtained

$$0000000 \quad 0111100 \quad 1100110 \quad 1010101$$

$$\left\{ \begin{array}{l} 1,000,000 \\ 88-58 \\ 1000,000 \\ 22-02 \end{array} \right. \quad \left\{ \begin{array}{l} 0101010 \\ 18-81 \\ 0011110 \\ 81-81 \end{array} \right. \quad \left\{ \begin{array}{l} 0110011 \\ 18-81 \\ 0110011 \\ 18-81 \end{array} \right. \quad \left\{ \begin{array}{l} 0000110 \\ 5-1 \\ 0101010 \\ 68-88 \end{array} \right. = 1$$

$$\left\{ \begin{array}{l} 1,000,000 \\ 88-58 \\ 1000,000 \\ 22-02 \end{array} \right. \quad \left\{ \begin{array}{l} 0011110 \\ 81-81 \\ 0001111 \\ 01-01 \end{array} \right. \quad \left\{ \begin{array}{l} 0110011 \\ 18-81 \\ 0011111 \\ 18-81 \end{array} \right. \quad \left\{ \begin{array}{l} 0101010 \\ 68-88 \\ 1010101 \\ 22-02 \end{array} \right. = 1$$

$$\left\{ \begin{array}{l} 0100000 \\ 58-58 \\ 0100000 \\ 22-02 \end{array} \right. \quad \left\{ \begin{array}{l} 1010101 \\ 18-81 \\ 0001111 \\ 01-01 \end{array} \right. \quad \left\{ \begin{array}{l} 0111001 \\ 18-81 \\ 0011100 \\ 18-81 \end{array} \right. \quad \left\{ \begin{array}{l} 1000011 \\ 5-1 \\ 1010101 \\ 22-02 \end{array} \right. = 1$$

RSA math

$$P=17, \quad q=11, \quad e=7, \quad M=88$$

$(88)^{\text{base } e} \pmod{n}$

$$n = p \times q = 17 \times 11 = 187$$

$$\phi(n) = (p-1) \times (q-1) = 16 \times 10 = 160$$

we know,

$$d = e^{-1} \pmod{\phi(n)}$$

$$\therefore d \times e \pmod{\phi(n)} = 1$$

$$\therefore (23 \times 7) \pmod{160} = 1$$

$$\therefore d = 23$$

NOW, encryption, $c = m^e \pmod{n}$

$$(88^4 \times 88^3) \pmod{187} = (88)^7 \pmod{187}$$

$$88^4 = 192 \pmod{187}$$

$$88^4 \pmod{187} = 132$$

$$88^3 \pmod{187} = 44$$

$$132 \times 44 = 5808 \pmod{187} = 11$$

- decryption, = $c^d \pmod{n}$

$$\equiv (11)^{23} \pmod{187}$$

$$(11) \times (11) \times (11) \times (11) \times (11) \times (11) \times (11) = 11 \times 11 = 121 \pmod{187}$$

$$(11)^9 = 33 \pmod{187}$$

$$(11)^{17} = 108 \pmod{187}$$

$$= (11)^9 \times (11)^9 \times (11)^9 \pmod{187}$$

$$= (33 \times 33 \times 108) \pmod{187}$$

$$= 88$$

Ans

$$L = (0.01) \text{ km} \times b.$$

$$L = (0.01) \text{ km} \times (8 \times 8)$$

$$L = 0.01 \text{ km}$$

$$(0.01) \text{ km} \times 64 = 0.64 \text{ km}$$

$$x 81 \text{ km} = 88$$

$$88 \text{ किमी } = 88$$

$$88 \text{ किमी } = 88 \text{ km}$$

$$88 \text{ km} = 88 \text{ km}$$

$$11 = 88 \text{ km} \times 0.01 = 88 \text{ km}$$

Diffie - Hellman math!

(ii) primitive root of 11 - forms words

$$(2) \mod 11 \text{ has } 2^3 \text{ (E)} =$$

$$(2)^2 \bmod 11 = 4$$

$$(2)^3 \bmod 11 = 8$$

$$(2)^{94} \bmod 11 = \underline{5} \text{ since } 2^2$$

$$(2)^5 \bmod 11 = 10$$

$$(2)^6 \bmod 11 = 9$$

$$(2)^x \mod 11 = x$$

$$(2)^8 \bmod 11 = 3$$

$$(2)^9 \bmod 111 = 6$$

$$(2)^{10} \mod 11 = 1$$

(ii) Here, A has public key, $y_A = 9$

So, A's private key $n_A = ?$

we know,

$$(y_p)^n \equiv a \pmod{p} \quad \text{and} \quad y_p^n \equiv a \pmod{q}$$

$$y_p = c^m (2)^{np} \pmod{11}$$

$$\Rightarrow g = (2)^{n_A} \mod 11 = \textcircled{6} \quad 2^6 \mod 11 \\ \therefore n_A = 6$$