

Assignment 1

$$(Q.1) \quad \text{Permutation } \pi : S \rightarrow S \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 13 & 5 & 6 & 9 & 11 & 01 & 81 & 2 & 10 \end{pmatrix} \quad \begin{pmatrix} 10 & 11 & 12 \\ 4 & 12 & 7 \end{pmatrix}$$

Plaintext : CRYPTOGRAPHY

(a) The transposition cipher were basically permuted the plaintext as per the given secret key, which is essentially a permutation π . The 1st row here represents position of the final decrypted text and the 2nd row represents those positions that would be used to construct the encrypted text.

For example,

$($	1	2	3	4	- - -	$)$
\downarrow	\downarrow	\downarrow	\downarrow	\downarrow	- - -	$)$
$\underline{3}$	$\underline{5}$	$\underline{6}$	$\underline{9}$	- - -		

This means, 3rd character of plaintext will become 1st character in encrypted text and so on.

Using this logic, encrypted text = YTOAHCRPPYQ

(b) Permutation π is basically a bijective mapping from set $S \rightarrow S$. [S = set of characters in plaintext] It is essentially a mapping and hence it is always invertible. (\because Bijections are invertible).

For decryption, we would use the following inverse permutation.

2021S1138

Sonidhya Kumar

CLASSMATE

Date _____

Page _____

for 1st row: $(1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12)$
for 2nd row: $(6 \ 8 \ 10 \ 12 \ 13 \ 12 \ 7 \ 8 \ 9 \ 5 \ 11)$

THURSDAY is the result

lets understand this mapping, this mapping means
that the 6th character from the cipher text
will become the 1st character in the decrypted
text and so on. It will map 6 to 1, 12 to 2, 10 to 3, 8 to 4, 11 to 5, 5 to 6, 13 to 7, 7 to 8, 9 to 9, 1 to 10, 2 to 11, 3 to 12.

Using this logic, decrypted text = CRYPTOGRAPHY

Text becomes after mapping of 1 to 6
 $(C \ R \ Y \ P \ T \ O \ G \ R \ A \ H \ Y)$

High frequency of characters like 'T' can be seen

Text becomes after mapping of 1 to 6
 $(C \ R \ Y \ P \ T \ O \ G \ R \ A \ H \ Y)$

so on

CRYPTOGRAPHY = Text happens upon with who?

permutation or mapping of different letters

Resultant arrangement is P_1, P_2, \dots, P_n for most

purpose of it need to cipher text in sequence of P_1, P_2, \dots, P_n

(addition of P_1, P_2, \dots, P_n)

Sequence will be called cipher text and message will

Q.2) Shift cipher is basically shifting each character of the plaintext by a fixed number of characters keeping in mind that it is mod 26.

So, Enc^(c)(x, k) = (x+k) mod 26 with the series
 and Dec^(c)(c, k) = (c+26-k) mod 26

x = plaintext

k = key (positions to be shifted)

$c = \text{ciphertext}$

It is important to note that $A=0$, $B=1$, \dots , $Z=25$.

Using this logic, ciphertext for WEAREINDIAN is -

from Wm. E. Farwell R. W. Ewing N. D. Johnson A. N.

$$\begin{array}{r} (22+4) \\ \hline 26 \end{array} \downarrow \quad \downarrow 11 \quad \downarrow 12 \quad \downarrow 11 \quad \downarrow \text{2nd box} \quad \downarrow 11 \quad \downarrow \text{3rd box} \quad \downarrow 1$$

Asplenium platyneuron L. var. *marinum* R.

Hence, ciphertext = AIEV'IMRH'MER

~~Xanthium strumarium~~ - fresh foliage and flowers

Now, let's decrypt using method defined above—

A I E V I M R H M E R
 $(0+26-4)$
W E A P P E S I N D I A N

Hence, decrypted text = **WE ARE INDIAN**

Hence, correct

Q.3) Plaintext: WEAREINDIAN at message time (s.o)

Secret Key: CRICKET and extending with 'X' at both ends of both strings

First of all, lets build the 5×5 playfair Matrix using all the rules of playfair cipher. ($I=J$)

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

Next step is to add a delimiter 'X' b/w repeated characters but since we do not have any repeated characters, we skip this step and move on to making length of plaintext even by adding a 'x' at last

\therefore Processed text = WEAREINDIANX

Now, lets break it into blocks of two :-

W	E	A	R	C	R	I	N	D	I	N	A	N	X
1	2	3	4	5	6	7	8	9	10	11	12	13	14

\therefore WEAREINDIANX = 14x14 matrix

Let us now encrypt it using the 5×5 matrix —

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

→ for blocks
1, 2, 3, 4

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

5, 6

∴ Ciphertext = ZR HACK MF RB LZ

let us now decrypt it using the rules for decryption
for playfair cipher & the 5×5 matrix —

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

ZR HA CK MF RB LZ
1 2 3 4 5 6

→ for blocks
1, 2, 3, 4

202151138

Sonidhya Kumar

861121509

classmate

Date _____
Page _____

C	R	K	E	O	I	A	N	T
T	A	D	B	D	F			
G	H	L	M	I	N			
O	P	Q	S	V	U			
V	W	X	Y	Z				
	0	1	2	3	4	5	6	7

∴ Decrypted text = [WEAREINDIANX]

We got our preprocessed string back, hence
verified playfair cipher!

0	1	2	3	4	5	6	7
8	9	0	1	2	3	4	5
6	7	8	9	0	1	2	3

[S I G R A M K U R B I S] = friendly :-

→ also softwares with python & c++ support available

→ function 2x2 with 8 input string only

2	3	8	5	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	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	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000

202151138

Sanidhya Kumar

classmate

Date _____

Page _____

Q.4) In Affine cipher, $K = (a, b)$ ————— $0 \leq a, b \leq 25$
 and $\text{Enc}(x) = (ax + b) \% 26$ at 0 odd

$$\text{as } b \equiv (1 \oplus a) + a(1 \oplus a)$$

In case of affine cipher, decryption is not possible when the key a is not relatively prime (co-prime) to 26. This means that a and 26 have a common factor other than 1. If a and 26 have a common factor, there exists some letters that cannot be decrypted unambiguously because multiple letters would map to the same ciphertext.

$$\text{gcd}(a, 26) \neq 1$$

The decryption algorithm for affine cipher is —

1. Find the modular multiplicative inverse of $a \% 26$.
 Let's denote this as a^{-1} .
2. Calculate $x = a^{-1} (y - b) \% 26$.

Here, the condition is $\text{gcd}(a, 26) = 1$.

Now, we have to find combination of a & b for which they will result same (x, y) for different keys, (a, b) and (a', b') .

$k_1 \neq k_2$ (fixed pair)

$$ax + b \equiv y \pmod{26} \quad \text{--- (1)}$$

$$a'x + b' \equiv y \pmod{26} \quad \text{--- (2)}$$

$$(a - a')x + (b - b') \equiv 0 \pmod{26} \quad \text{--- (3)}$$

As we know x can take any values b/w 0 to 25; let's say $x=0$; so if a

$(a-a') \cdot 0 + (b-b') \equiv 0 \pmod{26}$

$$(a-a') \cdot 0 + (b-b') \equiv 0 \pmod{26} \quad \text{--- (4)}$$

for all a & b , $(b-b') \equiv 0 \pmod{26}$ --- (4)

a & b' can also take any values b/w 0 to 25.

To satisfy eqn (4) let's $\rightarrow b' = b$

so eqn (4) becomes $(a-a')x \equiv 0 \pmod{26}$

so eqn (3) becomes $(a-a')x \equiv 0 \pmod{26}$

$$(a-a') \equiv 0 \pmod{26} \quad \text{--- (5)}$$

so $a' = a$ & $b' = b$

There are 12 possible values ($\gcd(a, 26) = 1$)

for a to satisfy eqn (5), $a \neq a'$ will be true

As $a' = a$ & $b' = b$ So $k_1 = k_2$

∴ Our assumption was wrong.

$d \neq b$ is a contradiction

So, for any values of (a, y) , two diff. keys never result in same pair of plaintext-ciphertext (x, y) .

① \rightarrow as $k_1 = k_2 \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

② \rightarrow as answer is 0 .

$$\Rightarrow \text{option } 0 = (d-a) + bc(d-a)$$

202151138

Sanchaya Kumar

classmate

Date _____

Page _____

Q.5) Given that $C_1 = \text{Enc}(m, k)$ and $C_2 = \text{Enc}(\bar{m}, k) = (1)$

where, Enc is encryption fn of DES.

$$x = (x_1, \dots, x_n)$$

$$\bar{x} = (1 \oplus x_1, 1 \oplus x_2, \dots, 1 \oplus x_n)$$

We have to find relation b/w C_1 and C_2 .

⇒ Case 1 - Complement as Normal Way -

The key scheduling algo produced round keys k_1, k_2, \dots, k_{15} while the complemented key scheduling algo produces round keys $\bar{k}_1, \bar{k}_2, \dots, \bar{k}_{15}$.

This complementation part is not affected by PC1, PC2 and left shift operations used in Enc. fn of DES. Let us jump into round fn. and see what happens there.

Consider the initial setup as follows:

\bar{m}

\bar{m}

L_0	R_0
-------	-------

i Got: $L_0 || R_0$

$\bar{L}_0 || \bar{R}_0$

L_1	R_1
-------	-------

To prove, $L_1 || R_1$ along $\bar{L}_1 || \bar{R}_1$ and $L_1 = R_0$

In the first round, $L_1 = R_0$

$$R_1 = L_0 \oplus f(R_0)$$

and $L_1 = \bar{R}_0$

$$\bar{R}_1 = \bar{L}_0 \oplus f(\bar{R}_0)$$

(A)

Let see what happens inside $f(\cdot)$

$$f(R) = f(R; k) = P(S(E(R_0) \oplus k))$$

Let's check f for \bar{R}_0 : $(\bar{x} \oplus k) = x$

$$(\bar{x} \oplus k) = (\bar{x} \oplus \bar{k}) = x$$

$$\therefore \text{then } f(\bar{R}_0) = f(\bar{R}_0, \bar{k})$$

$$\Rightarrow P(S(E(\bar{R}_0) \oplus \bar{k})) \leftarrow \text{from above}$$

$$\text{similarly } P(S(E(\bar{R}_0) \oplus \bar{k})) \because E(\bar{R}_0) = \bar{E}(R_0)$$

$$\text{also } P(S(E(\bar{R}_0) \oplus \bar{k})) \because \bar{A} \oplus \bar{B} = A \oplus B$$

This is actually $f(R_0)$

∴ L_0 becomes as follows

$$\begin{aligned} L_0 &= \sum_i f_i(\bar{R}_0) \\ &\Rightarrow \bar{L}_0 \oplus f(\bar{R}_0) \xrightarrow{\text{from above}} \\ &= \bar{L}_0 \oplus f(R_0) \quad \because \bar{A} \oplus B = A \oplus B \end{aligned}$$

$$\therefore L_0 = \bar{R}_0$$

∴ Therefore, after 1 round we get $\bar{L}_0 \parallel \bar{R}_1$

After 16 such rounds, final $\bar{L}_{16} \parallel \bar{R}_{16}$

Then again we apply IP_1 which has no effect and is also complemented.

Consequently, $C_1 = \bar{C}_2$ at the end.

2021S1138

classmate

Sonidhya Kumar

Date _____

Page _____

More clearly,

for $\text{Enc}(m, k)$ we get C_1 as $L_{16} \amalg R_{16}$ then

apply IP^T on C_1 matrix then

for $\text{Enc}(\bar{m}, \bar{k})$, we get C_2 as $L_{16} \amalg R_{16}$ then
apply IP^T

using this we can talk about effect of IP^T

as IP^T has no role it does not affect complement.

Therefore, finally, final conclusion

$$\text{Enc}(m, k) = C_1$$

$$\text{Enc}(\bar{m}, \bar{k}) = \bar{C}_1 = C_2$$

final conclusion.

$$\therefore C_1 = \bar{C}_2$$

\Rightarrow Case 2: Complement as per Sir's method given

in question. $\bar{x} = (1 \oplus x_1 \oplus \dots \oplus x_n - 1 \oplus \bar{x}_n)$

$$\text{We get, } x = \bar{x} \quad \therefore C_1 = C_2$$

$$\text{eg } x = 1010 \quad \text{with } \bar{x} = 1101$$

Sir's way
of defining.

Q.6) In Shift cipher, we have a plaintext which gets shifted character by character by a fixed key k .

Now, to decrypt the same, we shift each character in the opposite direction by same amount k . We will do this until we find a meaningful plaintext back (in case, we don't know k).

$$\text{Enc}(x, k) = (x+k) \% 26$$

$$\text{Dec}(x, k) = (x-k) \% 26$$

Note that $A=0, B=1, \dots, Z=25$ here, for x .

We will use brute force, that is, vary k from 1 to 25 until we get a meaningful decryption.

1) $k=1$ decryption

Ciphertext : AFITIFWE

Plaintext decrypted : ZEHSHHEVE

∴ decrypted text has no meaning, move forward

2) $k=2$ decryption

Ciphertext : AFITIFWE

decrypted : YDGRGDUD

202151138

Sawdhey Lemma

classmate

Date _____

Page _____

∴ decrypted text has no meaning, move forward.

3) $k=3$, decryption - \rightarrow ~~fixing the shift~~ \rightarrow ~~is having~~

Ciphertext : AFITIFWF ~~is having~~

decrypted : XCFQFC^TC

∴ decrypted text has no meaning, move forward.

4) $k=4$, decryption - \rightarrow ~~is having~~

Ciphertext : AFITIFWF ~~is having~~

decrypted : WBEPEBSB

∴ decrypted text has no meaning, move forward.

5) $k=5$, decryption - \rightarrow ~~is having~~

Ciphertext : AFITIFWF \rightarrow ~~is having~~

decrypted : VADODARA

∴ decrypted text makes sense and has a meaning,
we finally stop here. \rightarrow ~~J J J J = M~~

∴ Plaintext = VADODARA

Secret key = 5

2021S1138

Sandhyo

classmate

Data
Page

Q.7) In Hill Cipher, we have a secret key $A = (a_{ij})_{n \times n}$ such that A is invertible and $M = [m_1, m_2, m_3, \dots, m_n]$.

Hence, ciphertext $C = AM$

$$C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix}$$

Let's see, C and M now. Here given

$$M = \text{HILL} = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} 23 \\ 8 \\ 24 \\ 9 \end{bmatrix}$$

using the mapping $A = \Phi, B = 1, C = 2, \dots, Z = 25$

lets assume $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$

From matrix addition in A there are four eqns:

$$\rightarrow \begin{bmatrix} 23 \\ 8 \\ 24 \\ 9 \end{bmatrix} = \begin{bmatrix} a_{11} + a_{12} + a_{13} + a_{14} \\ a_{21} + a_{22} + a_{23} + a_{24} \\ a_{31} + a_{32} + a_{33} + a_{34} \\ a_{41} + a_{42} + a_{43} + a_{44} \end{bmatrix} \begin{bmatrix} 7 \\ 8 \\ 11 \\ 19 \end{bmatrix}$$

From this, we will get four eqns:-

$$7a_{11} + 8a_{12} + 11a_{13} + 11a_{14} = 23$$

~~7a₁₂ + 8a₁₃~~ ~~11a₁₄~~ is A tenth down

$$7a_{21} + 8a_{22} + 11a_{23} + 11a_{24} = 8$$

$$7a_{31} + 8a_{32} + 11a_{33} + 11a_{34} = 24$$

$$7a_{41} + 8a_{42} + 11a_{43} + 11a_{44} = 11$$

All eqns are under modulo 26, so we will add 26 to RHS since we are not getting solⁿ with this

$$7a_{11} + 8a_{12} + 11a_{13} + 11a_{14} = 49$$

$$7a_{21} + 8a_{22} + 11a_{23} + 11a_{24} = 34$$

$$7a_{31} + 8a_{32} + 11a_{33} + 11a_{34} = 50$$

$$7a_{41} + 8a_{42} + 11a_{43} + 11a_{44} = 35$$

Now, we will solve these eq's and find a solution such that A is invertible, there may be multiple solⁿs but we have to choose the one which is invertible. We have used online calculator for this since it is complicated. We get,

$$A = \begin{bmatrix} 0 & 2 & -1 & 3 \\ 1 & 2 & 1 & 0 \\ 1 & 4 & 0 & 1 \\ 0 & 3 & 0 & 1 \end{bmatrix}$$

2021S1138

Sonidhya

classmate

Date _____

Page _____

- method with diagram -

Q.8) (a) $\text{gcd}(222, 18)$ using Euclidean Algorithm -

$$18 \quad | \quad 222 \quad | \quad 12 \quad 12 - 5 \times 2 =$$

$$-18 \downarrow (5 \times 2 - 2 \times 1) \quad 5 \times 2 - 2 \times 1 =$$

$$42 \times 3 - 88 \times 2 =$$

$$-36 \quad | \quad 18 \quad | \quad 3 \quad \therefore \text{gcd}(222, 18) = 6$$

$$6 \quad | \quad 18 \quad | \quad 3$$

$$-18 \quad | \quad 3 \quad | \quad 0$$

$$0 \quad | \quad 3 \quad | \quad 0$$

(b) x_0, y_0 s.t. $1 = 33x_0 + 13y_0$ using Euclidean -

+ using Extended Euclidean Algorithm

$$\text{1} = (33, 13) \text{ O.P.}$$

$$13 \quad | \quad 33 \quad | \quad 2 \quad | \quad 0$$

$$-26 \quad | \quad 2 \quad | \quad 1 \quad | \quad 0$$

$$13 \quad | \quad 2 \quad | \quad 1 \quad | \quad 0$$

$$-7 \quad | \quad 1 \quad | \quad 0 \quad | \quad 0$$

$$\therefore \text{gcd}(13, 33) = 1$$

Now we will find x_0, y_0 such that $1 = 33x_0 + 13y_0$.

$$1 = 33(-2) + 13(1) \quad \text{and it is clear}$$

$$1 \quad | \quad 6 \quad | \quad 16$$

$$-2 \quad | \quad 6 \quad | \quad 0$$

$$3 \quad | \quad 0 \quad | \quad 0$$

$$2 \quad | \quad 1 \quad | \quad 0$$

Now, $\text{gcd}(x, y) = ax + by \rightarrow$ Using Bezout's Identity

Traceback in the division -

$$= 7 - (13) - 1 \times 7$$

$$= 2 \times 7 - 13$$

$$= 2 \times (33 - 2 \times 13)$$

$$= 2 \times 33 - 5 \times 13$$

$$\downarrow \quad \quad \quad \downarrow$$

This is of the form $ax + by$

$$\begin{cases} x_0 = q = 2 \\ y_0 = b = -5 \end{cases}$$

(c) Mul. inv. of 5 under mod 26

lets check if mult. inv. is possible or not

$$\gcd(5, 26) = 1$$

∴ possible

$$\text{Now, } 1 = 26 - 5 \times 5$$

According to Bezout's identity, $\gcd(x, y) = ax + by$
lets see -

By, extended euclidean algorithm as well

multiplicative inverse of 5 :-

$$\begin{array}{r} 5 \quad | \quad 26 \quad | \quad 5 \\ \underline{-25} \end{array}$$

$$\begin{array}{r} 1 \quad | \quad 5 \quad | \quad 5 \\ \underline{0} \end{array}$$

2021S1138

Sanihya

classmate

Date _____

Page _____

$$1 = 5x + 26y \rightarrow \text{Bezout's identity.}$$

$$1 = 1 \cdot 26 - 5 \cdot 5$$

\therefore Multiplicative inverse of 5 under mod 26 = -5
 \because It is mod 26, we add 26 to -5 to
 make it positive
 $-5 + 26 = 21$

Therefore, mul. inv. of 5 under mod 26 = 21

$$\begin{array}{r} \text{LHS} \quad (1+x+^2x+^3x+^4x) \\ \times (-5+^2x+^3x+^4x+^5x) \\ \hline (1+^2x+^3x+^4x+^5x) \\ + x(-5+^2x+^3x+^4x) \\ = -5+^2x+^3x+^4x+^5x \end{array}$$

$$\begin{array}{r} x \left[(1+^2x+^3x+^4x+^5x) + (-5+^2x+^3x+^4x+^5x) \right] \\ = x(1+^2x+^3x+^4x+^5x) \\ = x + ^2x + ^3x + ^4x + ^5x \end{array}$$

Q.9) Input = $[D_3]_{16}$

Output = 66

Convert D_3 to polynomial form.

$$[D_3]_{16} = [1 \ 10 \ 0 \ 0 \ 11]_2$$

$$\therefore \text{Polynomial} = x^7 + x^6 + x^4 + x + 1$$

$$(S = DS + D)$$

Find inverse of $x^7 + x^6 + x^4 + x + 1$ under

$$[S] = DS \bmod x^8 + x^4 + x^3 + x + 1$$

$$x^7 + x^6 + x^4 + x + 1 \quad | \quad x^8 + x^4 + x^3 + x + 1 \quad | \quad x + 1$$

$$(-) \underline{x^8 + x^7 + x^5 + x^2 + x}$$

$$x^7 + x^5 + x^4 + x^3 + x^2 + 1$$

$$(-) \underline{x^7 + x^6 + x^4 + x + 1}$$

$$x^6 + x^5 + x^3 + x^2 + x$$

$$x^6 + x^5 + x^3 + x^2 + x \quad | \quad x^7 + x^6 + x^4 + x + 1 \quad | \quad x$$

$$(-) \underline{x^7 + x^6 + x^4 + x^3 + x^2}$$

$$x^3 + x^2 + x + 1 \quad | \quad x^6 + x^5 + x^3 + x^2 + x + 1$$

$$(-) \underline{x^6 + x^5 + x^4 + x^3}$$

$$x^4 + x^2 + x$$

$$(-) \underline{x^4 + x^3 + x^2 + x}$$

$$x^3$$

$$(-) \underline{x^3 + x^2 + x + 1}$$

$$x^2 + x + 1$$

$$(100x^2 + x + 1) \left| \begin{array}{r} x^3 + x^2 + x + 1 \\ x^3 + x^2 + x \\ \hline \end{array} \right. \quad |$$

Note:

All under q. 2

$$\text{Now, } 1 \neq (x^3 + x^2 + x + 1) + (x)(x^2 + x + 1)$$

$$\Rightarrow (x^3 + x^2 + x + 1) + x \{ (x^6 + x^5 + x^3 + x^2 + x) +$$

$$\{ (x^5 + x + 1) (x^3 + x^2 + x + 1) \}$$

$$\Rightarrow (x^3 + x^2 + x + 1) (x^4 + x^2 + x + 1) + x (x^6 + x^5 + x^3 + x^2 + x)$$

$$\Rightarrow \{ (x^7 + x^6 + x^4 + x + 1) + x (x^8 + x^5 + x^3 + x^2 + x) \}$$

$$\downarrow \quad \cdot (x^4 + x^2 + x + 1) + x (x^6 + x^5 + x^3 + x^2 + x)$$

P(x)

$$\Rightarrow P(x) (x^4 + x^2 + x + 1) + (x^6 + x^5 + x^3 + x^2 + x) (x^5 + x^3)$$

$$\Rightarrow P(x) (x^4 + x^2 + x + 1) + (x^6 + x^5 + x^3 + x^2 + x) (x^5 + x^3)$$

$$\Rightarrow P(x) (x^4 + x^2 + x + 1) + \{ (x^8 + x^4 + x^3 + x + 1) + P(x) \}$$

$$\Rightarrow Q(x) (x^5 + x^3 + x^2) + P(x) \{ (x^5 + x^3 + x^2) (x + 1) + (x^4 + x^2 + x + 1) \}$$

$$\Rightarrow (x^5 + x^3 + x^2) Q(x) + (x^6 + x^5 + x + 1) P(x)$$

Form is satisfied

$$\therefore \text{Inverse} = P(x) = x^6 + x^5 + x + 1$$

$$\text{In Binary} = [01100011]_2$$

$$\therefore S(11010011) = 01100011$$

Q.10) Given $\rightarrow 33, 42, 66, 24$ at frame word

First step is converting each of them to their binary

$$33 = (00100001)_2 \rightarrow x^5 + 1$$

$$42 = (00101010)_2 \rightarrow x^5 + x^3 + x^2$$

$$66 = (01000010)_2 \rightarrow x^6 + x$$

$$24 = (00011000)_2 \rightarrow x^4 + x^3$$

lets say output is x, y, z, w

$$\begin{array}{|c|} \hline \text{All under mod } x^8 + x^4 + x^3 + x + 1 \\ \hline \end{array}$$

$$\begin{aligned} x &= x(x^5+1) + (x+1)(x^5+x^3+x) + x^6+x+x^4+x^3 \\ &= x^6 + x + x^6 + x^4 + x^2 + x^5 + x^5 + x^6 + x + x^6 + x^4 + x^3 \\ &= x^6 + x^5 + x^2 + x \end{aligned}$$

$$\begin{aligned} y &= x^5 + 1 + x(x^5+x^3+x) + (x+1)(x^6+x) + x^4 + x^3 \\ &= x^5 + 1 + x^6 + x^4 + x^2 + x^7 + x^2 + x^6 + x + x^4 + x^3 \\ &= x^7 + x^5 + x^3 + x + 1 \end{aligned}$$

$$\begin{aligned} z &= x^5 + 1 + x^5 + x^3 + x + x(x^6+x) + (x+1)(x^4+x^3) \\ &= x^5 + 1 + x^5 + x^3 + x + x^7 + x^2 + x^5 + x^4 + x^6 + x^4 + x^3 \\ &= x^7 + x^5 + x^2 + x + 1 \end{aligned}$$

$$\begin{aligned} w &= (x+1)(x^5+1) + x^5 + x^3 + x + x^6 + x + x(x^4+x^3) \\ &= x^6 + x + x^6 + 1 + x^7 + x^3 + x + x^6 + x + x^5 + x^4 \\ &= x^5 + x^4 + x^3 + x + 1 \end{aligned}$$

Date _____

Page _____

Now, convert to binary \rightarrow E8E4A4AD (0110)

$$\text{or } y = x^6 + x^5 + x^2 + x \rightarrow 01100110 \rightarrow 102$$

$$y = x^7 + x^5 + x^3 + x + 1 \rightarrow 10101011 \rightarrow 171$$

$$z = x^7 + x^5 + x^2 + x + 1 \rightarrow 10100111 \rightarrow 167$$

$$w = x^5 + x^4 + x^3 + x + 1 \rightarrow 1001110111 \rightarrow 59$$

$$x + \bar{x} \leftarrow (01000010) = 30$$

$$\therefore \text{AES Mix Column } (33, 42, 66, 24) = \underline{(102, 171, 167, 59)}$$

W.E.B. V. distinction MOD 269

$$(x^6 + x^5 + x^3)x + (x^6 + x^5 + x^2)(1+x) + (1+x^2)x = 0$$

$$x^7 + x^6 + x^3 + x^5 + x^4 + x^2 + x + x^3 + x^2 + x^6 = 0$$

$$x^7 + x^5 + x^4 + x^3 + x^2 + x = 0$$

$$(x^6 + x^5 + x^3)(1+x) + (x^6 + x^5 + x^2)x + 1+x^2 = 0$$

$$x^7 + x^6 + x^4 + x^3 + x^2 + x + x^5 + x^4 + x^3 + x^2 + x^6 = 0$$

$$x^7 + x^5 + x^4 + x^3 + x^2 + x = 0$$

$$(x^6 + x^5 + x^3)(1+x) + (x^6 + x^5)x + x^7 + x^6 + x^4 + x^2 + x^6 = 0$$

$$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + x^6 + x^5 + x^4 + x^3 + x^2 + x^6 = 0$$

$$x^7 + x^5 + x^4 + x^3 + x^2 + x = 0$$

(Q.11)

 $P \rightarrow \text{prime number } a, b \in \mathbb{Z}_p$

$$f(a, b) : \mathbb{Z}_p \rightarrow \mathbb{Z}_p \quad f(a, b)(x) = (ax + b) \bmod p$$

$$\forall x \neq x' \in \mathbb{Z}_p, f(a, b)(x) = y \quad f(a, b)(x') = y'$$

$$f(a, b)(x') = y'$$

$$(ax + b) \equiv y \bmod p \quad \text{--- (A)}$$

$$(ax' + b) \equiv y' \bmod p \quad \text{--- (B)}$$

$$(A) - (B)$$

$$a(x - x') \equiv (y - y') \bmod p$$

$$a \equiv (y - y')(x - x')^{-1} \bmod p$$

$$x - x' \neq 0 \text{ as } x \neq x' \rightarrow \text{Given}$$

So, for checking if we can find a and b
 we need to check if $(x - x')^{-1}$ exists or not.
 i.e., if $(x - x')$ is invertible or not under \mathbb{Z}_p .

Inverse of $(x - x')$ w.r.t p exists iff $\gcd(x - x', p) = 1$

As $p \rightarrow \text{prime no.} \Rightarrow \gcd(x - x', p) = 1$

\therefore Inverse of $(x - x')$ w.r.t p exists.

So, we can find a and b .

For a — $\left(\frac{q}{p} \right) \text{ is adjoins sumg } \left(\frac{p}{q} \right)$ (1.8)

$q \text{ bsm } \left(\frac{p}{q} \right) \Rightarrow a \equiv (y' - y)(x' - x) \vdash q \vdash p \left(\frac{p}{q} \right) \text{ bsm}$
 Put this value of $(\frac{p}{q})$ in (A) and (B) to find b
 $b = (10)(10) \vdash$

Hence, we can derive a, b.

$$(A) \rightarrow q \text{ bsm } \frac{p}{q} \equiv (d + x)$$

$$(B) \rightarrow q \text{ bsm } \frac{p}{q} \equiv (d + x)$$

$$\frac{p}{q} \vdash (A)$$

$$q \text{ bsm } \left(\frac{p}{q} \right) \equiv (x - x)$$

$$q \text{ bsm } \left(\frac{p}{q} \right) \equiv (x - x)$$

Now $\left(\frac{p}{q} \right) \vdash \text{ he } \neq x \text{ so } 0 \neq x - x$

d has a long run w/ 0's which is not so.

There is always $\left(\frac{p}{q} \right)$ if $x \neq 0$ at least one

get values for $\left(\frac{p}{q} \right)$ which are not $\left(\frac{p}{q} \right)$ if $x \neq 0$

$\left(\frac{p}{q}, x - x \right)$ bsm iff $p \vdash (x - x)$ in 323M

$\left(\frac{p}{q}, x - x \right)$ bsm iff $p \vdash (x - x) \neq 0$

202151138

Saniidhya

classmate

Date _____

Page _____

A.12) Hash function $h : (Z_2)^7 \rightarrow (Z_2)^4$
 $h(x) = xA$

$$x \in \{-1, 1\}^7 \iff x \in \{0, 1\}^7$$

To find all pre-images of $[0 \ 1 \ 0 \ 1]$

$$x \in \{0, 1\}^7$$

$$x = [x_1 \ x_2 \ x_3 \ x_4 \ x_5 \ x_6 \ x_7]$$

(SOP form) provides $x \in \{0, 1\}^7$

$$[x_1 \ x_2 \ x_3 \ x_4 \ x_5 \ x_6 \ x_7] \left[\begin{array}{c|ccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right]$$

$$= \text{and } \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\} = \{0, 1\}$$

$$\text{and } \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{and } h(x) = xA \iff h(x) = x \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = [0 \ 1 \ 0 \ 1]$$

$$\text{and } h(x) = xA \iff h(x) = x \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = [0 \ 1 \ 0 \ 1]$$

$$\begin{bmatrix} x_1 + x_2 + x_3 + x_4 + x_1 \\ x_2 + x_3 + x_4 + x_5 \\ x_3 + x_4 + x_5 + x_6 \\ x_4 + x_5 + x_6 + x_7 \end{bmatrix}^T = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}^T$$

$$\therefore \text{Eqns} \rightarrow x_1 + x_2 + x_3 + x_4 = 0 \quad \text{--- A}$$

$$x_2 + x_3 + x_4 + x_5 = 1 \quad \text{--- B}$$

$$\text{and } x_3 + x_4 + x_5 + x_6 = 0 \quad \text{--- C}$$

$$\text{and } x_4 + x_5 + x_6 + x_7 = 1 \quad \text{--- D}$$

$$A \rightarrow B \Rightarrow x_1 = x_5 + 1 \rightarrow E$$

$$B \rightarrow C \Rightarrow x_2 = x_6 - 1 \rightarrow F$$

[Eq 10] Positioning the half of

$$C \rightarrow D \Rightarrow x_3 = x_7 + 1 \rightarrow G$$

As all x_i are binary (since φ_2)

From eqn D it is clear that one x_i out of (x_4, x_5, x_6, x_7) will be = 1

— OR —

any three x_i out of (x_4, x_5, x_6, x_7) will be = 1

So, all possible cases are listed below :-

$$(x_4, x_5, x_6, x_7) = \{ (0, 1, 1, 1), (1, 0, 1, 1), \\ (1, 1, 0, 1), (1, 1, 1, 0), \\ (0, 0, 0, 1), (0, 0, 1, 0), \\ (0, 1, 0, 0), (1, 0, 0, 0) \}$$

By looking at eqns E, F, G we can find values of x_1, x_2, x_3 :-

A C Code was used to implement this tedious task (took permission from sir).

2021/11/38

Soni Dhyey

classmate

Date _____

Page _____

Therefore, all possible preimages of $(0,1,0,1)$ are as follows:

1. $(0, 0, 0, 0, 1, 1, 1)$

2. $(1, 0, 0, 1, 0, 1, 1)$

3. $(0, 1, 0, 1, 1, 0, 1)$

4. $(0, 0, 1, 1, 1, 1, 0)$

5. $(1, 1, 0, 0, 0, 0, 1)$

6. $(1, 0, 1, 0, 0, 1, 0)$

7. $(0, 1, 1, 0, 1, 0, 0)$

8. $(1, 1, 1, 0, 0, 0, 0)$

(1) and (8) are same

$$(x)_{cd} = (c)_{cd}$$

$$[(c)_{cd} \parallel (c)_{cd}]_{id} = [(c)_{cd} \parallel ((c)_{cd})_{id}]_{id}$$

9

If f is a function mapping from A to B , then f is surjective if every $b \in B$ has at least one $a \in A$ such that $f(a) = b$.

(Q.13)

$$h_1 : \{0, 1\}^{2m} \leftrightarrow \{0, 1\}^m$$

\hookrightarrow Collision Resistant Function.

$$h_2 : \{0, 1\}^m \rightarrow \{0, 1\}^m$$

TP — h_2 is collision resistant

Assume h_2 is not collision resistant

\therefore There exists x and x'

such that $x \neq x'$

$$\text{and } h_2(x) = h_2(x')$$

$$\left. \begin{array}{l} x = x_1 || x_2 \\ \text{and } x' = x'_1 || x'_2 \end{array} \right\} \begin{array}{l} \text{all } x_1, x_2, x'_1, x'_2 \\ \in \{0, 1\}^m \end{array}$$

$$h_1 \left[\underbrace{h_1(x_1) || h_1(x_2)}_{\alpha} \right] = h_1 \left[\underbrace{h_1(x'_1) || h_1(x'_2)}_{\beta} \right]$$

We know h_1 is collision resistant \therefore it is difficult to find α and β such that $\alpha \neq \beta$

$$\text{and } h_1(\alpha) = h_1(\beta)$$

$$\therefore \alpha = \beta$$

202151138

Sandhya Kumar

classmate

Date _____

Page _____

$$\Rightarrow h_1(x_1) \parallel h_1(x_2) = h_1(x_1') \parallel h_1(x_2')$$

$$\text{So, } h_1(x_1) = h_1(x_1')$$

$$h_1(x_2) = h_1(x_2')$$

We know h_1 is collision resistant

$$\text{so, } x_1 = x_1'$$

$$x_2 = x_2'$$

" We say $\boxed{x = x'}$

But this is a contradiction to our assumption that $x \neq x'$.

Hence, proved by contradiction that h_2 is also collision resistant function.