Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber2 dev - CFA CCI Avignon

15 février 2024

Chiffrements par transposition

ordre des lettres du texte clair est modifié

- Chiffrement à dents de scie
- Scytale
- Cas général
- Chiffrement par transposition de colonnes

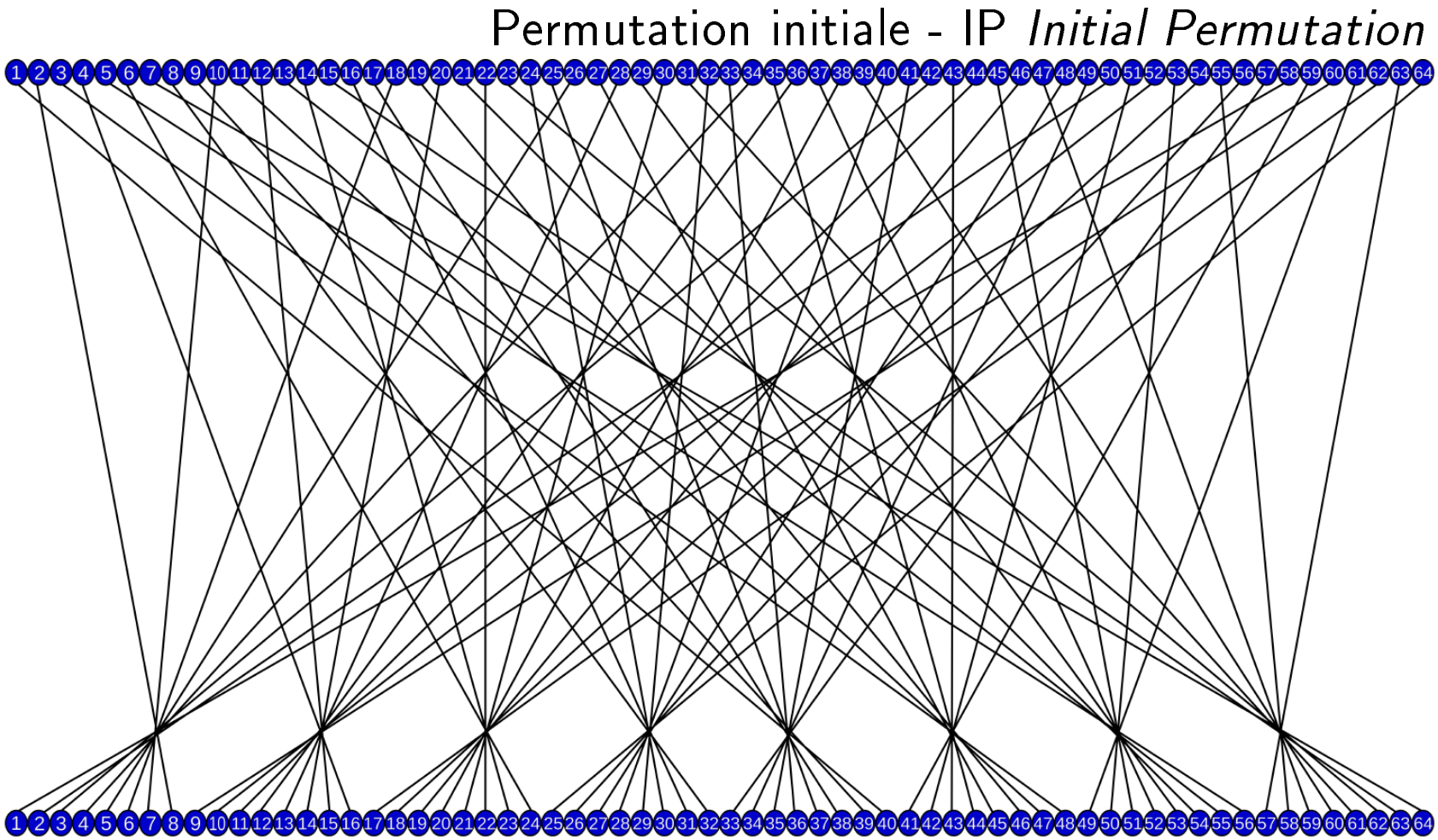
Transposition - permutation

transposition définie par une permutation sur un bloc de taille donnée.

Exemple: permutation [3, 6, 5, 1, 4, 2]

clair	1	2	3	4	5	6
	S	E	C	R	E	T
chiffré	3	6	5	1	4	2
	C	T	E	S	R	E

exemple: dans le chiffrement DES



source: wikipedia

exemple: dans le chiffrement DES

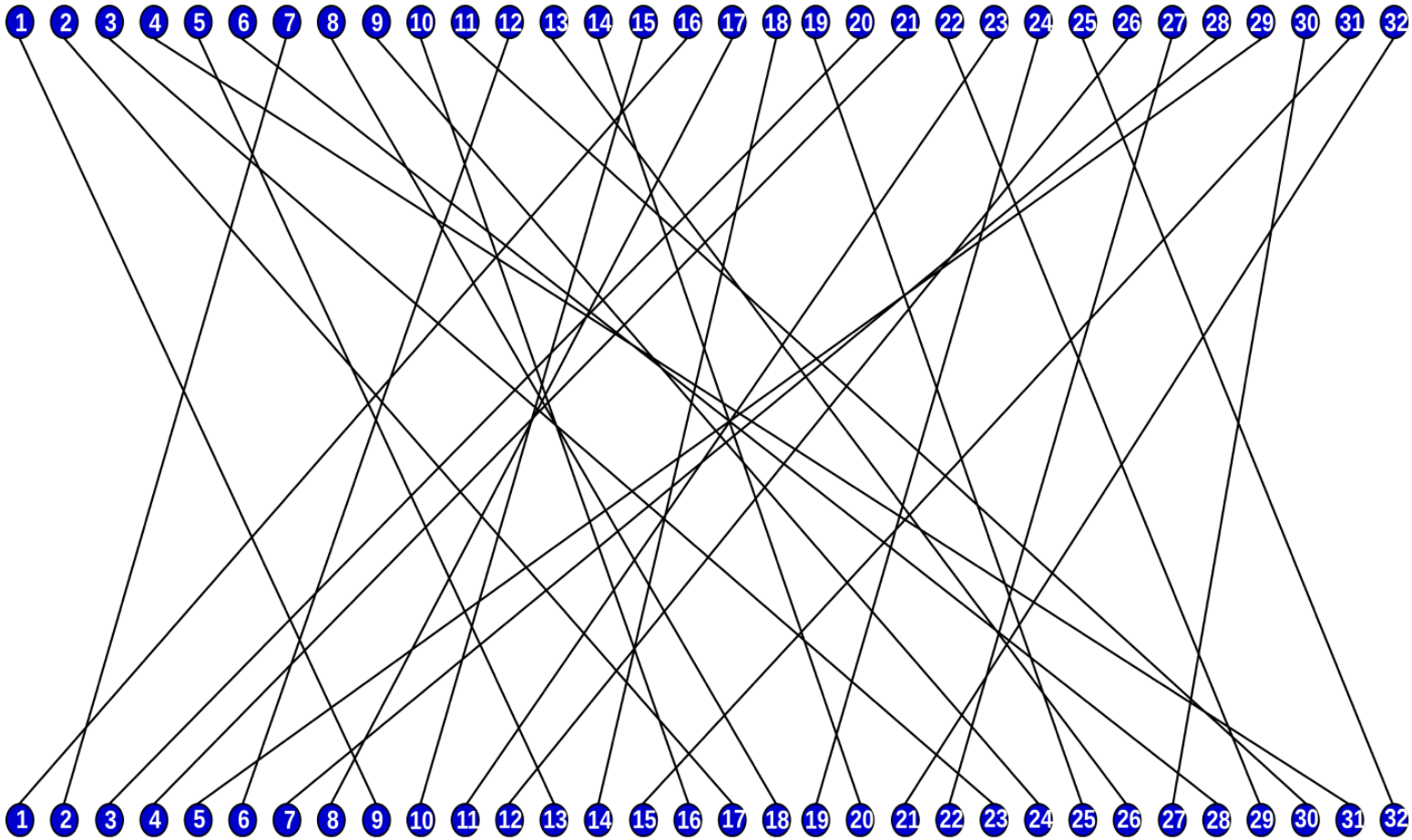
permutation donnée sous forme de tableau:

premier bit de sortie provient du 58ème bit d'entrée
second bit provient du 50ème...

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

exemple: dans le chiffrement DES



source: wikipedia

permutation inverse

clair	1	2	3	4	5	6
	S	E	C	R	E	T
chiffré	3	6	5	1	4	2
	C	T	E	S	R	E
déchiffré	4	6	1	5	3	2
	S	E	C	R	E	T

exemple: dans le chiffrement DES

fonction inverse de la permutation initiale IP^{-1} (ou FP pour final permutation) donnée par le tableau:

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Chiffrement par transposition par permutation de colonnes

1	2	3	4
M	E	S	S
A	G	E	S
U	P	E	R
S	E	C	R
E	T	X	X

devient

3	4	2	1
S	S	E	M
E	S	G	A
E	R	P	U
C	R	E	S
X	X	T	E

Chiffré: SEECXSSRRXEGPETMAUSE

Permutation inverse

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad \text{devient} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

1	2	3	4
S	S	E	M
E	S	G	A
E	R	P	U
C	R	E	S
X	X	T	E

déchiffré

4	3	1	2
M	E	S	S
A	G	E	S
U	P	E	R
S	E	C	R
E	T	X	X