TÀI LIỆU THAM KHẢO

MẬT THƯ

MẬT THƯ

CÁC DẠNG MẬT THƯ CƠ BẢN

HƯỚNG DẪN GIẢI MẬT THƯ

GIẢI MẬT THƯ

MẬT THƯ TRÒ CHƠI LỚN

NHỮNG VẤN ĐỀ CƠ BẢN VỀ MẬT THƯ

MẬT THƯ - MORSE - SEMAPHORE

MẬT THƯ-Trần Thời

ĐĨA QUAY 3 TẦNG GIẢI MẬT THƯ

MẬT THƯ – Nguyễn Minh Hoàng Hải

MỘT SỐ KHÁI NIỆM

Thư viện Online 102

CHÚNG TA THƯỜNG NGHĨ:	NHƯNG CHÍNH XÁC LÀ:
MẬT THƯ	
Là một **lá thư** bí mật.	Là một **bản tin** viết dưới dạng bí mật
Được **quy định** trước với nhau.	Được **quy ước** giữa 2 người hoặc 2 đơn vị với nhau.
Là cách **sắp xếp** các mẫu tự, các tiếng…	Là **cách thể hiện** các trật tự khác thường
Làm theo yêu cầu của nội dung lá thư	**Thực hiện** nội dung của bản tin

MỘT SỐ KHÁI NIỆM

CHÚNG TA THƯỜNG NGHĨ:	NHƯNG CHÍNH XÁC LÀ:
MẬT MÃ	
Là một mật thư.	Là những quy tắc, quy ước riêng dùng để thay đổi hình thức biểu hiện thông tin.
Giải mã là tìm các cách sắp xếp các mẫu tự, các tiếng…	Giải mã là cách khám phá các trật tự khác thường
Giải mã nhằm thấy được nội dung lá thư	Giải mã nhằm thể hiện nội dung của bản tin
Mật mã gồm 2 yếu tố: hệ thống và chìa khóa.	

MỘT SỐ KHÁI NIỆM

Thư viện Online 102

GIẢI MÃ	
Là các bước của quá trình khám phá những bí mật: *ký hiệu, cách sắp xếp…* để biết được nội dung bản tin.	Xác định hệ thống.
	Đi tìm chìa khóa.
	Mã hóa nội dung bản tin.
	Thiết lập các mẫu tự, các tiếng, các câu…
	Thực hiện nội dung bảng mã.

MỘT SỐ KHÁI NIỆM

Thư viện Online 102

CHÌA KHÓA

Là phần gợi ý của người soạn (viết), giúp cho người giải (đọc) đoán biết hệ thống và tìm ra qui luật nhất định để giải mã.	Ký hiệu: hình cái chìa khóa 🗝 hoặc viết OTT, O=n, On Chìa khóa được đặt ra nhằm mục đích là để nâng cao tính bí mật của bản tin. Nếu là mật thư đơn giản thì không cần thiết phải có chìa khóa.

MỘT SỐ KHÁI NIỆM

Thư viện Online 102

HỆ THỐNG

Là những qui định bất biến các bước tiến hành trong việc sử dụng các ký hiệu và cách sắp xếp.	Có 3 hệ thống: - Hệ thống thay thế. - Hệ thống dời chỗ. - Hệ thống ẩn giấu.

MẬT THƯ

Các Hệ thống

Dời chỗ — **Trật tự** các mẫu tự được **dịch chuyển** hoặc **xáo trộn**

Ẩn giấu — Bản tin được đưa **thêm ký tự lạ** vào để giấu nội dung.

Thay thế — Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

HỆ THỐNG DỜI CHỖ

Dời chỗ — **Trật tự** các mẫu tự được **dịch chuyển** hoặc **xáo trộn**

OTT: Gió thổi theo hướng Đông Bắc.

✉ :

C	**U**	**B**	**T**	**F**
H	**S**	**J**	**H**	**N**
C	**N**	**N**	**O**	**R**
A	**A**	**O**	**A**	**Y**
H	**C**	**G**	**X**	**Z**

HỆ THỐNG DỜI CHỖ

Dời chỗ Trật tự các mẫu tự được **dịch chuyển** hoặc **xáo trộn**

OTT: Gió thổi theo hướng Đông Bắc.

Đông Bắc

✉ :

C	U	B	T	F
H	S	J	H	N
C	N	N	O	R
A	A	O	A	Y
H	C	G	X	Z

=> CHUCS BANJ THANHF COONG ARXYZ

=> CHÚC BẠN THÀNH CÔNG

HỆ THỐNG ẨN GIẤU

OTT: "Bước ra một bước một dừng
Trông xa nàng đã tỏ chừng nẻo xa" (Kiều)

✉ : CẢ ĐỘI AI NÀO MÀ ĐẾN CHỖ ĐÍCH VỀ TRƯỚC THÌ SẼ CÓ ĐƯỢC MƯỜI MỘT QUẢ NÃI TRÁI CHUỐI BOM

Ẩn giấu Bản tin được đưa **thêm ký tự lạ** vào để giấu nội dung.

HỆ THỐNG ẨN GIẤU

OTT: "Bước ra một bước một dừng
Trông xa nàng đã tỏ chừng nẻo xa" (Kiều)

⊠ : ĐỘI NÀO ĐẾN ĐÍCH TRƯỚC
SẼ ĐƯỢC MỘT NÃI CHUỐI

Ẩn giấu Bản tin được đưa **thêm ký tự lạ** vào để giấu nội dung.

HỆ THỐNG THAY THẾ *(số thay chữ)*

OTT: A = 1.
⊠ **: 20, 9, 5, 5, 14, 19 – 12, 5, 5, 14**

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã **Thay thế**

HỆ THỐNG THAY THẾ *(số thay chữ)*

OTT: A = 1.

⌧ **: 20, 9, 5, 5, 14, 19 – 12, 5, 5, 14**

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

=> TIEENS LEEN

=> TIẾN LÊN

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

HỆ THỐNG THAY THẾ *(chữ thay chữ)*

OTT: A = d.

⌧ **: QER – ALKG - IBBRC**

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

HỆ THỐNG THAY THẾ *(chữ thay chữ)*

OTT: A = d.

⌧ : **QER – ALKG - IBBRC**

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
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

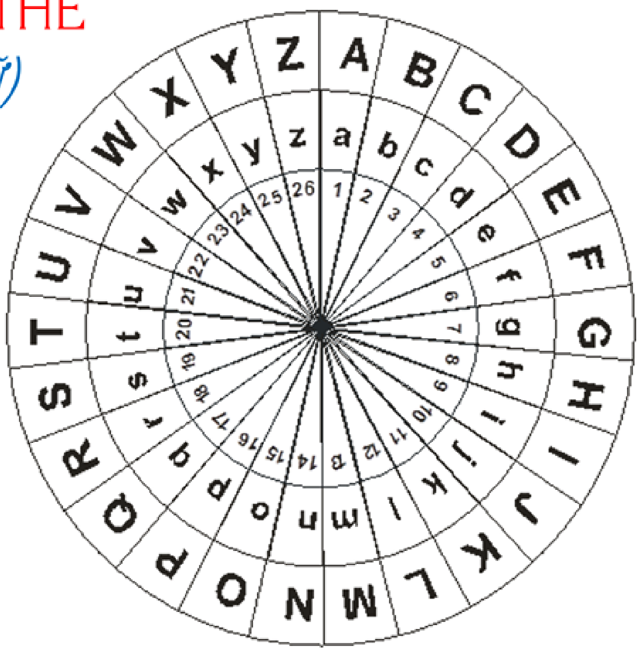
=> thu – donj – leeuf

=> thu dọn lều

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

ĐĨA GIẢI MẬT THƯ THAY THẾ
(chữ thay chữ, số thay chữ)



Một số THUẬT NGỮ dùng trong hệ thống THAY THẾ

Thư viện Online 102

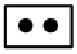
KÝ TỰ	THUẬT NGỮ THAY THẾ	KÝ TỰ	THUẬT NGỮ THAY THẾ
A	Người đứng đầu (Vua, anh cả,..), át xì, ây	G	Gờ, ghê, gà
B	Bò, Bi, 13,...	H	Hắc, đen, thang, hờ, hát
C	Cê, cờ, trăng khuyết	I	cây gậy, ia, ai, số một
D	Dê, đê	J	Dù, gi, móc, boy, nặng
E	e thẹn, 3 ngược, tích	K	Già, ca, kha, ngã ba số 2
F	ép, huyền	L	En, eo, cái cuốc, lờ

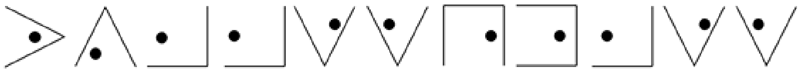
Một số THUẬT NGỮ dùng trong hệ thống THAY THẾ

Thư viện Online 102

KÝ TỰ	THUẬT NGỮ THAY THẾ	KÝ TỰ	THUẬT NGỮ THAY THẾ
M	Em, mờ, ...	T	Tê, Ngã ba số 1, te
N	Anh, nờ, ...	U	Mẹ, you
O	Trăng tròn, bánh xe, cái miệng, trứng, miệng giếng...	V	Vê, vờ, Hai
P	Phở, phê, chín ngược	W	Oai, kép, anh em song sinh
Q	Cu, rùa, quy, ba ba, bà đầm	X	Cây kéo, ích, ngã tư
R	Hỏi,	Y	Ngã ba số 3
S	Ech, Việt Nam, hai ngược	Z	Kẻ ngoại tộc, anh nằm, co

HỆ THỐNG THAY THẾ *(ký hiệu thay chữ)*

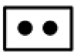
OTT: 

✉ : 

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

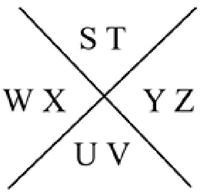
HỆ THỐNG THAY THẾ *(ký hiệu thay chữ)*

OTT: 

✉ : 

Chuồng bò:

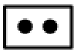
A B	C D	E F
G H	I J	K L
M N	O P	Q R

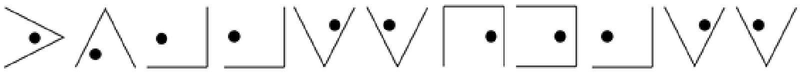


Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

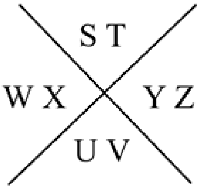
HỆ THỐNG THAY THẾ *(ký hiệu thay chữ)*

OTT: 

✉ : 

Chuồng bò:

A B	C D	E F
G H	I J	K L
M N	O P	Q R



=> XUAATSPHATS

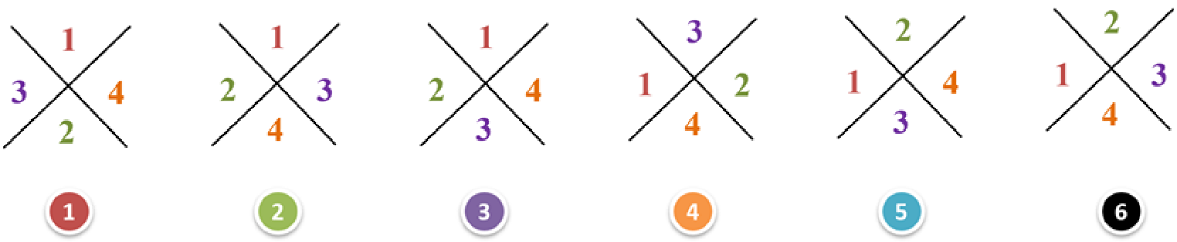
=> XUẤT PHÁT

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

HỆ THỐNG THAY THẾ *(ký hiệu thay chữ)*

Lưu ý: Nếu đặt ST = 1; UV = 2; WX = 3; YZ = 4, ta có **6 cách** thể hiện khung 2:



Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

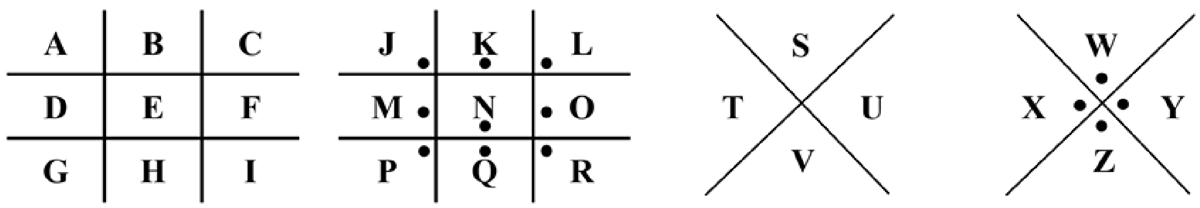
Thư viện Online 102

CÁCH SOẠN MẬT THƯ

CÁC BƯỚC SOẠN	VÍ DỤ MINH HỌA
Bước 1: Xác định nội dung cần mã hóa, Chuyển nội dung sang Quốc ngữ điện tín.	VÌ ĐÀN EM THÂN YÊU => **VIF DDANF EM THAAN YEEU**
Bước 2: Chọn hệ thống mã hóa nội dung.	Ta chọn hệ thống **Ẩn giấu**
Bước 3: Tiến hành mã hóa nội dung theo hệ thống đã chọn.	**V**2**I**56**F**1-78**D**5**D**7**A**3**NF**2-**E**57**M**1-2**T**3**H**54**A**3**A**0**N**-12**Y**6**E**7**EU**8
Bước 4: Chọn khóa để gợi ý cho việc giải mã mật thư.	Ai còn tập đếm thì cho ra ngoài.
Bước 5: Ghi lại mật thư hoàn chỉnh.	OTT: Ai còn tập đếm thì cho ra ngoài. ✉: V2I56F1-78D5D7A3NF2-E57M1-2T3H54A3A0N-12Y6E7EU8.

HỆ THỐNG THAY THẾ *(ký hiệu thay chữ)*

Chuồng heo:



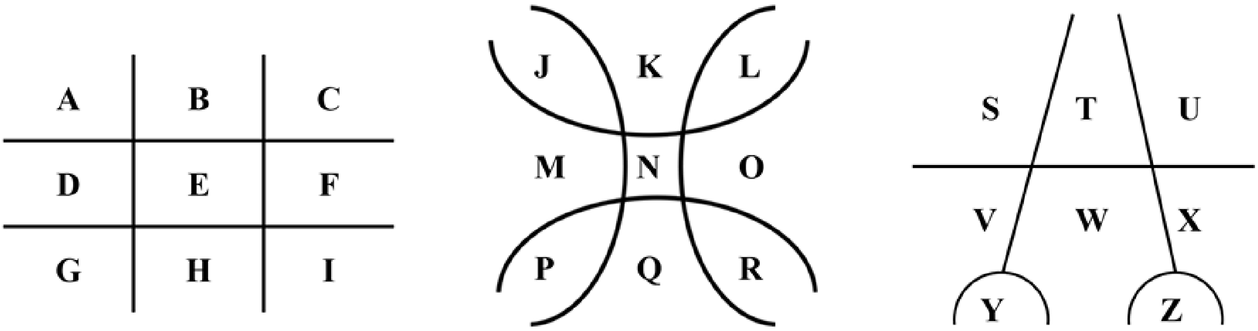
Thư viện Online 102

Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã

Thay thế

HỆ THỐNG THAY THẾ *(ký hiệu thay chữ)*

Chuồng bồ câu:



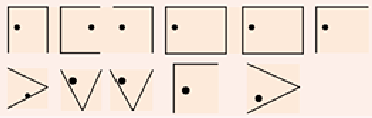
Mỗi mẫu tự của bản tin được **thay thế bằng một ký hiệu** mật mã **Thay thế**

CÁCH GIẢI MẬT THƯ

CÁC BƯỚC GIẢI	VÍ DỤ MINH HỌA
OTT: NHẢY CÓC. ✉: DADIOGAHNXF – TKHAATNAH4 – NGIUEDECN	
Bước 1: Xác định hệ thống mã hóa của mật thư.	B1: Đây là mật thư được mã hóa bằng hệ thống **Ẩn giấu**.
Bước 2: Trình bày cách giải mã.	B2: Theo chìa khóa, ta sẽ lấy 1 ký tự và bỏ 1 ký tự như kiểu **nhảy cóc**.
Bước 3: Giải mã nội dung.	B3: Ta có **nội dung** bản tin là: DDOANF – THANH - NIEEN
Bước 4: Ghi lại bạch văn hoàn chỉnh.	B4: => ĐOÀN THANH NIÊN

BÀI TẬP MẬT THƯ

Thư viện Online 102

ĐỀ	ĐỀ
1. OTT: X = (21/7) + 5 ✉: **NW/. 06.05.19 – 18.25.13.20 /AR** **2. OTT: Con Gà nó gáy ...** ✉: **NW/. CAFZK – LZSSQX /AR**	**6. OTT:**  ✉: 
3. OTT: Em hát – Anh ca ✉: **NW/. OCV – PYEEXN /AR** **4. OTT: Lưng vào trước** ✉: **NW/. GNÔC – HNÀHT - NẠB – CÚHC /AR**	**7. OTT: Thân em như chiếc thuyền trôi dạt** **Sóng xô ra rồi sóng lại đưa vào** ✉: **NW/. Hãy trưa về để gấp nấu nhóm** **Nay trở ăn trại cơm rồi lửa /AR**
5. OTT: Đầu chưa có - thừa ra đuôi ✉: **NW/. HIEEUSN – IEENT – IEENFP – HONGS – AWNXS – ANGFT /AR**	**8. OTT: Không được dùng thuốc ASPIRINE** ✉: **NW/. TAHU – DSONJ – LEPEUF – TIRAIJ –TRONWR – VEEFE /AR**

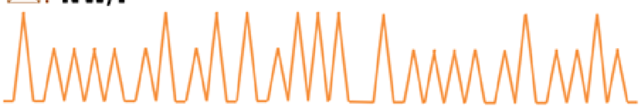
BÀI TẬP MẬT THƯ

Thư viện Online 102

ĐỀ	ĐỀ
9. OTT: " Được ngọc" đừng chia cho ai. ✉: **NW /. ỷk - mệin – óhk – nêuq /AR** **10. OTT: Em nào còn học ABC...xếp hàng cho ra về.** ✉: **NW /. TAINBHF – CBADNEJ – TFHAGATJ – HTRIONG – JSAKNGLS /AR.**	**12 . OTT: Một hàng dọc tập hợp : Bé trước Lớn sau** ✉: **NW /. Bồ câu PHAPS - Khủng long TRA – Trâu BIJ – Chó THUOWNG – Kiến OON – Voi KIEEMS – Vi khuẩn HAYX – Dê CHUAANR – Bướm PHUOWNG - Ruồi TAAPJ - Vịt CUWUS / AR.**
11. OTT: Một sống một chết. ✉: **NW /. XIN CHO CÁC ĐỒNG ĐỘI LÀM CHO NHÀ CỬA VÀ LỀU CHỐNG QUAY TRỞ VỀ BỐN HƯỚNG VIỆT NAM / AR.**	**13. OTT: Trăng già rồi đến trăng non** **Lòng thiếp vẫn mãi sắc son đợi chàng** ✉: **NW /. CAC – SOD – DOI – JCO – WRO – LAI – JCT – RON – GOL – EEU – FCC – HOW – FOL – EEN – HJC /AR.**

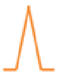
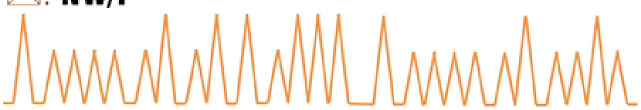
BÀI TẬP MẬT THƯ
(dùng tín hiệu Morse)

Thư viện Online 102

ĐỀ	ĐỀ
1. OTT: Nguyên tích - Phụ tè ✉: **NW/. gaiu + it + Kelu + oie - aiou + zkh + bmn + aohi /AR**	**4. OTT:** :  = te,  = tích ✉: **NW/.**  **/AR**
2. OTT: Chứng minh : tích = x và te = y ✉: **NW/. yxx + yxx + xx - xxxx + yyy + yxyx + xyxy /AR**	
3. OTT: Cao tè, Thấp tích ✉: **NW/. Loki + htp + te – lx + dtm + thb + al + bo /AR**	

BÀI TẬP MẬT THƯ
(dùng tín hiệu Morse)

Thư viện Online 102

ĐỀ	ĐỀ
1. OTT: Nguyên tích - Phụ tè ✉: **NW/. gaiu + it + Kelu + oie - aiou + zkh + bmn + aohi /AR**	**4. OTT:** :  = te,  = tích ✉: **NW/.**  **/AR**
2. OTT: Chứng minh : tích = x và te = y ✉: **NW/. yxx + yxx + xx - xxxx + yyy + yxyx + xyxy /AR**	
3. OTT: Cao tè, Thấp tích ✉: **NW/. Loki + htp + te – lx + dtm + thb + al + bo /AR**	

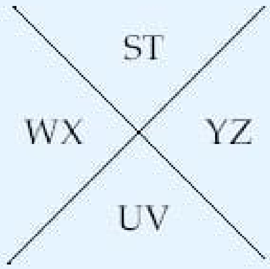
Hệ thống bảng tra

có sẵn do người truyền và người nhận thống nhất với nhau.

(a) Mật thư chuồng bò

Căn cứ vào vị trí các chuồng để tìm chữ cái

AB	CD	EF
GH	IJ	KL
MN	OP	QR



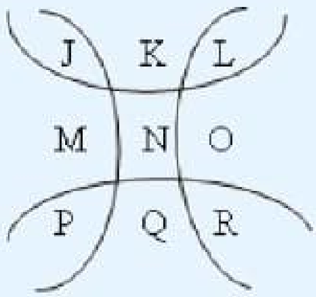
Thí dụ: O=n 

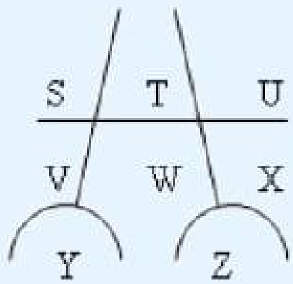
Tin 

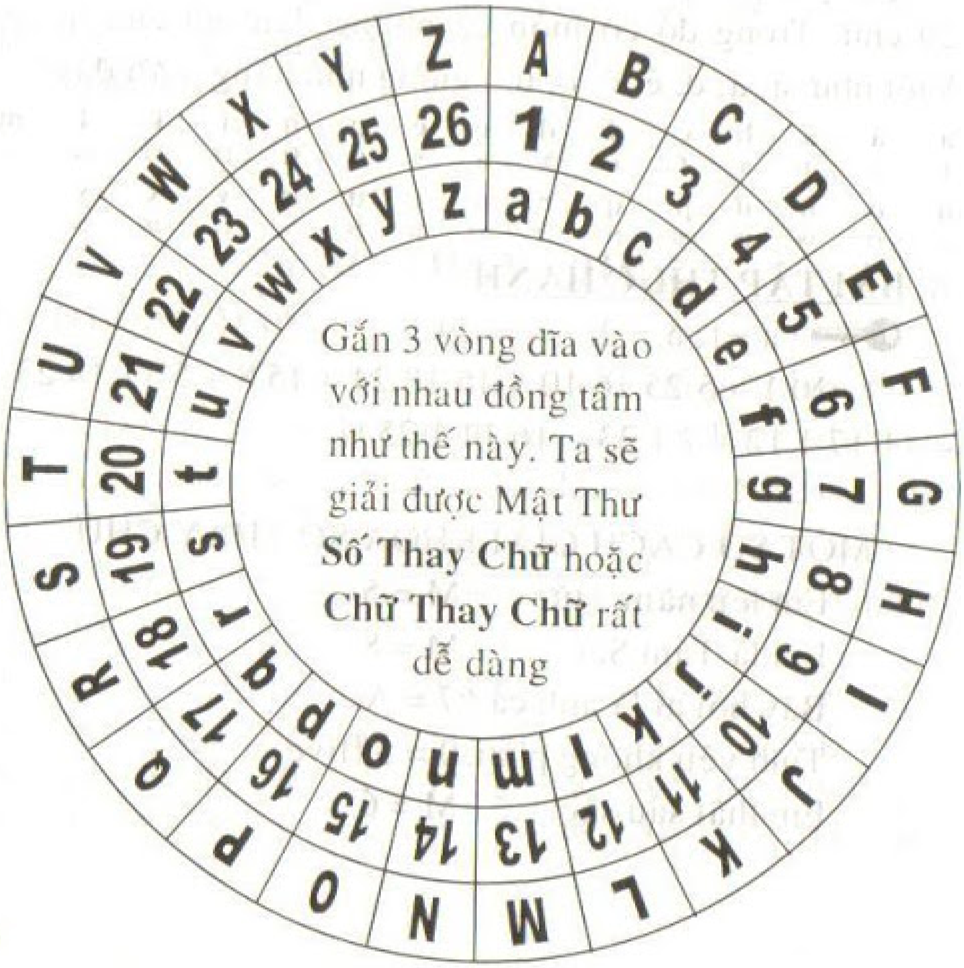
Giải C A W M S C O W Q

(b) Mật thư chuồng bồ câu

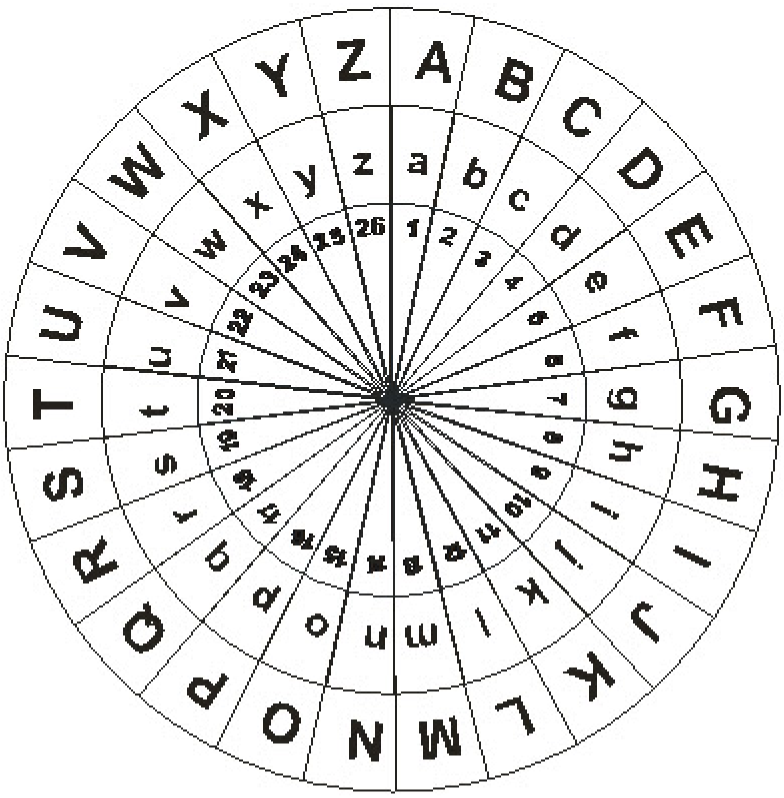
A	B	C
D	E	F
G	H	I







Gắn 3 vòng đĩa vào
với nhau đồng tâm
như thế này. Ta sẽ
giải được Mật Thư
Số Thay Chữ hoặc
Chữ Thay Chữ rất
dễ dàng


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
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
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26