

MẬT THƯ

Là một bức thư được viết dưới dạng bí mật. Nhằm giữ kín nội dung mà giữa người gửi và người nhận cần trao đổi.

Mật thư thường có 2 phần:

1) Bản mật mã

Là những ký tự hoặc hình vẽ, thoạt đầu có vẻ rất khó hiểu. Sau khi nghiên cứu kỹ chìa khóa, ta sẽ tìm ra hướng giải bằng cách đối chiếu những dữ kiện mà chìa khoá đã gợi ý.

2) Chìa khóa

Là một hình thức gợi ý cho người dịch tìm ra hướng giải mật thư. Chìa khóa có thể là một câu thơ hoặc một ký hiệu nào đó bằng hình vẽ. Ký hiệu của chìa khóa là: O=n

Sau khi giải mã xong, ta sẽ được một bản văn hoàn chỉnh, ta gọi đó là:

Bạch văn:

Là một văn bản hoàn chỉnh, tức là sau khi dịch xong, ta viết ra thành một bức thư bình thường mà ai cũng có thể đọc được.

Cách Giải Mã Mật Thư

- 1) Phải hết sức bình tĩnh
- 2) Tự tin nhưng không được chủ quan
- 3) Nghiên cứu khóa giải thật kỹ
- 4) Đặt các giả thiết và lần lượt giải quyết
- 5) Đối với việc giải mật thư trong trò chơi lớn, ta nên sao y bản chính và chia thành nhiều nhóm nhỏ để dịch. Như thế, ta sẽ tận dụng được hết những chất xám trí tuệ ở trong đội. Tránh tình trạng xúm lại, chụm đầu vào tranh dành xem một tờ giấy để rồi kết quả không đi tới đâu, mà dễ làm rách tờ giấy mật thư của chúng ta nữa.
- 6) Cuối cùng, nếu dịch xong, ta viết lại bản bạch văn cho thật rõ ràng, sạch sẽ và đầy đủ ý nghĩa.

Mật thư là những thông tin truyền đạt được mã hóa buộc người giải phải suy đoán mới giải được. Mật thư có thể chia làm 4 hệ thống:

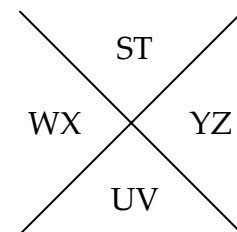
1) Hệ thống bảng tra


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

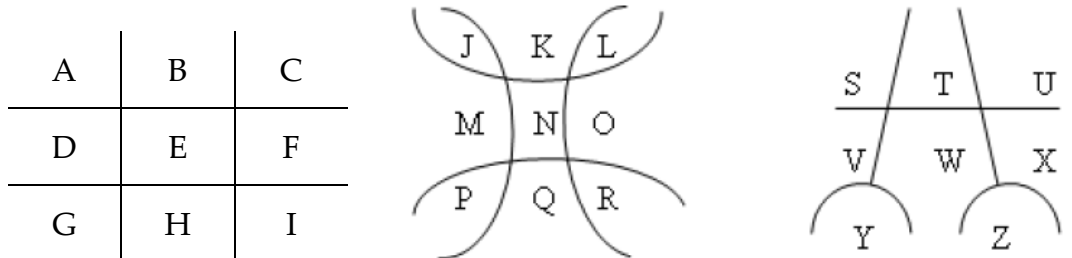


Thí dụ: O=n 

Tin 

Giải C A W M S C O W Q

(b) Mật thư chuồng bồ câu



2) Hệ thống thay thế

dựa vào dạng mật thư của Caesar. Mỗi mẫu tự bản văn được thay thế bằng một ký hiệu nào đó.

⇒ Nhận diện: mật thư viết toàn bằng chữ hoặc số (không có nghĩa)

eg. 1, 8, 22, 3/AR hay 010802203-132020/AR hay kzp-ccnnmfi/AR

⇒ Dịch mật thư:

- i) Giải khóa. Tìm xem số hoặc chữ cái đã cho ứng với chữ cái nào trong bảng chữ cái tiếng anh (26 chữ)
- ii) Thay khóa tìm được vào bảng chữ cái theo thứ tự
- iii) Căn cứ vào bản tin và bảng chữ cái để tìm các chữ cái phải tìm
- iv) Ráp các chữ cái tìm được thành chữ có nghĩa

(a) Dạng chữ thay chữ

Có nghĩa là một chữ trong bản tin được mã hóa bởi một chữ khác.

Thí dụ: O=n Một bảng hai

Tin e², p², d, k – m, b², q, k

Giải Một bảng hai là: A bằng 1, B bằng 2 (đứng thứ tự trong bản chữ cái. 1 = 2 tức là A = B

Thế vào bảng chữ cái:

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
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
e ² ,	p ² ,	d,	k	–	m,	b ² ,	q,	k																	
DD	OO	C	J	–	L	AA	P	J																	

Các chìa khóa thường thấy như:

- i) Cô người Hếu, mẹ người Bắc (nghĩa là O = U)
- ii) Anh bằng tuổi em (nghĩa là N = M)
- iii) Em đi chăn dê (nghĩa là M = D)

- iv) Bò con ngấm trắng (nghĩa là $B = O$)
- v) Đội trưởng đi với anh thứ sáu (nghĩa là $A = F$)
- vi) Hát hay không bằng hay hát (nghĩa là $H = K$)

(b) Dạng số thay số

một chữ trong bản tin được mã hóa bởi một con số, một dãy số khác.

Thí dụ: $O=n$ Trăm năm Kiều vẫn là Kiều

Tin 2, 1, 1, 20, 19 / 11, 8, 1, 21, 20, 19 / AR

Giải Khóa nghĩa là A vẫn đứng đầu, tức là A bằng 1, B bằng 2 (đúng theo thứ tự). Thế vào dãy số gồm 26 số:

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
2,	1,	1,	20,	19 /	11,	8,	21,	1,	20,	19															
B	A	A	T	S /	K	H	U	A	T	S															

Các chìa khóa thường thấy như:

- i) Áo em ba màu (nghĩa là $M = 3$)
- ii) Mươi bảy bé gãy sừng Trâu (nghĩa là $T = 17$)

3) Hệ thống dời chỗ

là hệ thống mà trong đó bản tin được mã hóa bằng cách di chuyển nội dung bản văn ie. không dùng ký hiệu mật mã nhưng nó xáo trộn trật tự bản tin.

Thí dụ 1: $O=n$ CAMRANH

Tin RWOIZ – NCLAF – TOTVE – ROQLF – EIOQF – TAAOF – EQISF

Giải Ta thấy có 7 cụm chữ và khóa cũng có 7 ký tự. Cách giải phụ thuộc vào việc dời những cụm chữ vào vị trí thích hợp để ra bản văn. Ta đặt cụm RWOIZ là cụm 1 và cứ thế đến cụm thứ 7 là EQISF. Khóa ta có chữ CAM RANH, ta chọn ký tự A của chữ CAM là 1 (vì đứng đầu bảng chữ cái). Ký tự A của chữ RANH là 2 và cứ thế cho đến 7. Sau đó ta lập bảng sau:

C	A	M	R	A	N	H
3	1	5	7	2	6	4
T	R	E	E	N	T	R
O	W	I	Q	C	A	O
T	O	O	I	L	A	Q
V	I	Q	S	A	O	L
E	Z	F	F	F	F	F

TRÊN TRỜI CAO TÔI LÀ VÌ SAO LẺ

