Crypto

Robert R. Enderlein

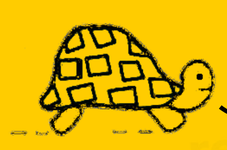
Easy: Find the permutation

There are five cables, hence 5! = 120 possible permutations.
Find the correct one…

- Using brute force and checks (manual or automatic)
- Using linguistic insights (letter frequencies, letter combinations, single-character words, diphtongs, …)
- Start with the diagonal entries (a,g,n,t,z)

	.1	.2	.3	.4	.5
1.	a	b	c	d	e
2.	f	g	h	i	k
3.	l	m	n	o	p
4.	q	r	s	t	u
5.	v	w	x	y	z

Medium: Reverse the encryption

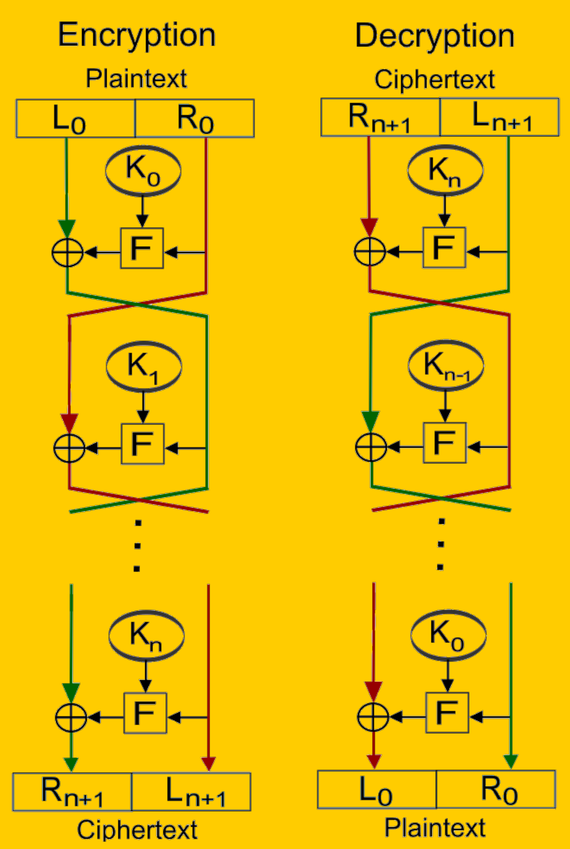


Encrypt every possible plaintext, and check whether the ciphertext is obtained
⇒ on average 2^{15} encryptions

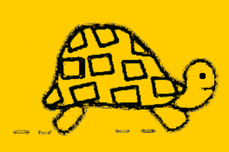
Observe how the encryption works.

Run the loop backwards: For each round i

- $R_i = L_{i+1}$
- $L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$



Hard: Crack the system



Try out every possible pair of keys K_1, K_2
Check whether encrypt(P, K_1, K_2) = C
Needs 2^{31} trials on average

Meet-in-the-middle attack: encrypt(P, K_1, K_2) = C ⇔ encrypt(P, K_1) = decrypt(C, K_2)

- Precompute intermediate cyphertexts for all 2^{16} K_1, store them in a hashmap
- Try out all 2^{16} K_2, and see whether a match is found in the hashmap

Needs on average $2^{16.58}$ calls to encrypt, and some map lookups