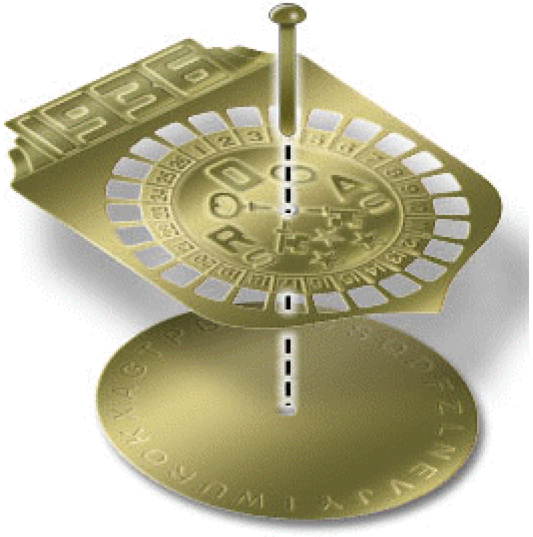
Encryption 101

Beyond the Secret Decoder Ring

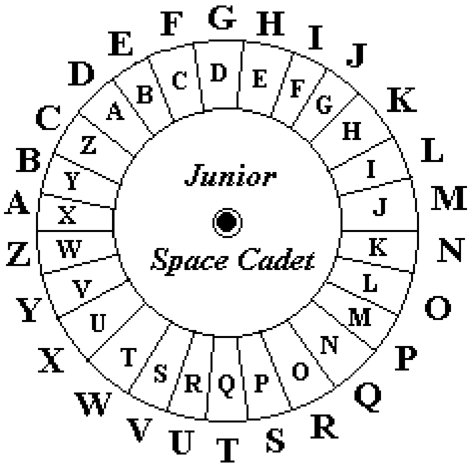
Sam Wagstaff
Computer Sciences and CERIAS

What is a secret decoder ring?



Popular 1930s to 1990s
Little Orphan Annie radio show
The image shown is from 1936
Also in breakfast cereal boxes

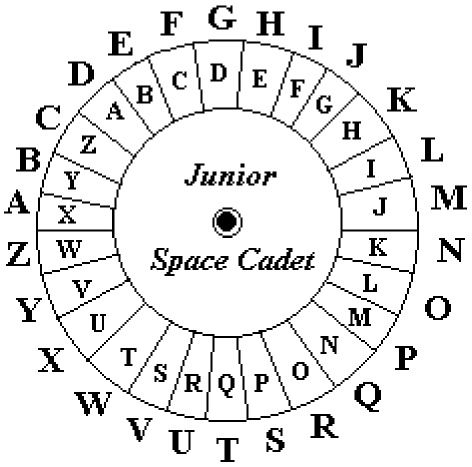
Another secret decoder ring


Junior
Space Cadet
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
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

Captain Midnight and the Space Cadets, radio and television

Also in breakfast cereal boxes

Most were badges, none was a ring

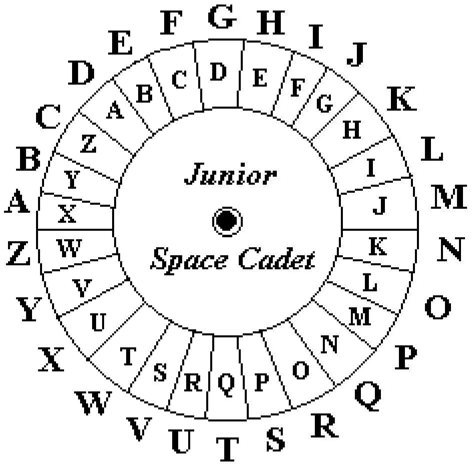


Plaintext or clear text – you can understand it
Ciphertext – looks like gibberish, but is equivalent to plaintext
Encipher or encrypt – convert plaintext to ciphertext using a key
Decipher or decrypt – convert ciphertext to plaintext using a key

The key for the secret decoder is the position of the alphabet circles.
The inner circle is the alphabet for plaintext.
The outer circle is the alphabet for ciphertext.

Example: plaintext: D R I N K
ciphertext: G U L Q N

A secret decoder does “clock arithmetic,” in fact, arithmetic modulo 26.

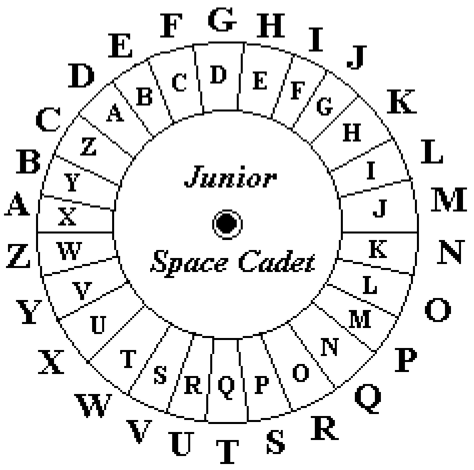

Junior
Space Cadet
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

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
0	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

Encipher by adding 3 to a plaintext letter’s value:
T + 3 = W, H + 3 = K, E + 3 = H,
so THE becomes WKH.
Decipher by subtracting 3 from a ciphertext letter’s value.

This cipher is also called a Caesar cipher.

To “break” a cipher means to either find the key or convert ciphertext to plaintext without knowing the key.



A Caesar cipher is easy to break because there are only 26 possible keys, and one can try all of them.

A secret decoder is adequate for secrets of Junior Space Cadets, but not for secrets of adults.

Ciphers are used for secret communication or for protecting secret files.

Cryptography is the study of ciphers.

Cryptanalysis studies how to break ciphers.

A slightly better cipher than a Caesar cipher is a cryptogram.

This is a simple substitution cipher in which the mapping from plaintext alphabet to ciphertext alphabet is an arbitrary permutation of the letters of the alphabet.

The number of possible keys is 26! = 403291461126605635584000000,

which is more keys than one could try in the lifetime of the universe.

Nevertheless, cryptograms appear as amusements each day in the *Exponent* and *Journal & Courier*. Many readers solve them every day.

Break it by guessing words from their letter patterns, or by using the relative frequency of individual letters. E is most frequent, T is second, etc.

Here is an example.

MVAG **SGVSXG** UTWG T

WGEGGL OUTO KVAGM **VII**

GTMHXF PHOU T **XHOOXG**

TXKVUVX. --- S. UTLLHMVE

  O   E   PEOPLE   E

MVAG **SGVSXG** UTWG T

    E   EE   O   E   O

WGEGGL **OUTO** KVAGM **VII**

E   L   L   L E

GTMHXF PHOU T **XHOOXG**

  L   O OL   P.   O

TXKVUVX.   --- S. UTLLHMVE

Types of Attacks on Ciphers

- Ciphertext only – Given only the ciphertext find the key and/or the plaintext.
- Known-plaintext attack – Given the ciphertext and corresponding plaintext, find the key.
- Chosen-plaintext attack – Cryptanalyst may **choose** some plaintext and learn the corresponding ciphertext. Goal: find key.

Types of Ciphers

- One key = Private key = Symmetric key

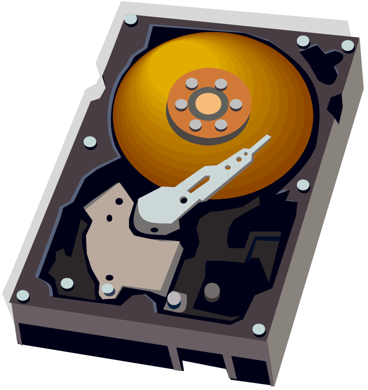
All mean that the same key is used to encipher and decipher. (Or else you can easily compute either key from the other.)

Has direct authentication

Uses bit manipulation

Very fast – At disk transfer rates

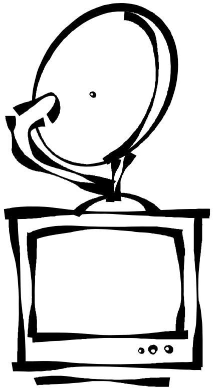
Examples: DES, AES



Common Symmetric Ciphers

DES has a 56-bit key. One can try all possible keys in < 1 day with special hardware. Differential cryptanalysis might help break it, too.

DES is used for short-term secrets, like satellite TV codes or press releases.



Common Symmetric Ciphers

AES has a choice of 128, 192 or 256-bit keys. It takes too long to try all possible keys, and there is no known better attack.

AES is used for serious secrets.

Types of Ciphers

- Two key = Public key = Asymmetric key

Enciphering key is public

Deciphering key is private (secret)

You must solve a hard problem to find the other key, give one of the two keys.

Has no direct authentication, but one can sign

Uses number theory and large integer arithmetic

Much slower than one-key ciphers

Examples: RSA, ElGamal, Rabin-Williams

Suppose Alice wants to email a long secret letter to Bob, but they haven’t agreed on a secret key for AES.

Alice uses a random AES key to encipher the letter and sends the ciphertext to Bob.

Alice enciphers the random key using Bob’s public RSA key and sends it to him.

Bob deciphers the second message with his secret RSA key and gets the AES key which he uses to decipher the letter.

Zimmermann’s PGP does all this and more.

Public key cryptography enjoys nice properties useful in complicated protocols, such as contract signing, electronic elections, oblivious transfer, digital cash and simultaneous exchange of secrets.

Traditional PKC uses exponentiation modulo a very large integer n, of 1024 bits or about 300 decimal digits.

Fast exponentiation makes these operations feasible, but still quite slow.

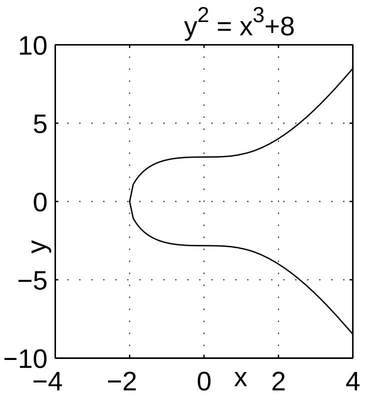
Traditional PKC operates in the multiplicative group of integers modulo n.

It assumes that one of these number theory problems is hard:

1. Factoring integers: Given n, find p and q with n = p*q.
2. Discrete logarithm: Given n, a and b, find e so that a raised to the e power is congruent to b modulo n.

The best known methods can solve either problem for n up to 200 decimal digits.

Elliptic curves



They provide many examples of mathematical groups for which the discrete logarithm problem is as hard using 128 bit numbers, or 40 decimal digits, as it is modulo n when n has 1024 bits, or 300 decimal digits.

This gives equal security faster, but still not as fast as symmetric ciphers.

Elliptic curves have other nice properties, too, that facilitate certain protocols.

Key Management

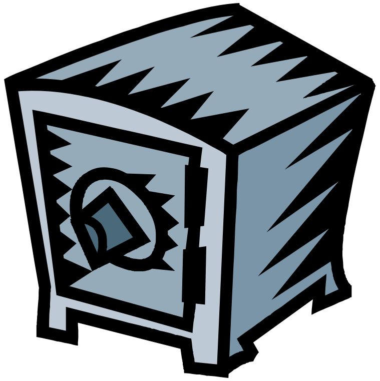
Modern encryption will secure your files and messages.

There is little danger anyone will find your key by brute force.

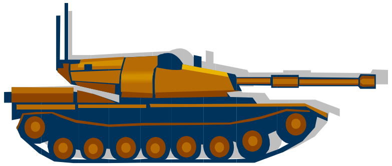
A greater danger is key loss.

Where do you store your key?

What if you lose your key?



Politics



- Strong cryptography cannot be exported.
- In law it is a munition, like a nuclear bomb.
- However, you may import cryptography.
- It is widely available on foreign web sites.
- Cryptography is restricted in several countries.