Lecture 2, Sept 26, 2001

- Review
- Vigenere Cipher
- Some history
- Algebraic Structures

An Important Distinction

Encryption = maintaining information secret/confidential

Authentication = proving and maintaining information integrity

Cryptography can be used at different levels

- algorithms: e.g. encryption algorithms, signature algorithms, hash algorithms
- protocols: between 2 or more parties, e.g., key distribution, fair exchange, authentication/login
- systems: e.g. electronic cash systems, smartcard systems
- attacks - on all the above

Some applications of cryptography

- network, operating systems security
- protect Internet, phone communications
- electronic payments
- database security
- software protection
- pay television
- military communications
- voting

Open versus closed system design

- **Open design**: algorithm, protocol, system design (and even possible plaintext) may be public information. The only secret is the key(s)

- **Closed design**: as much information as possible is kept secret

Types of Security

- unconditional or “information theoretic”: the security is provable/evident free of assumptions

- reducible or “provable”: one can prove that the security is as valid as some common, yet unproven, assumption

- ad hoc: the security seems good

Take a look at:

http://www.io.com/~ritter/GLOSSARY.HTM

The Vigenere Cipher

Related Primitive Ciphers

(all fairly weak)

- Shift: $Enc_k(x) = x+k \mod 26$
- Affine: $Enc_{k1,k2}(x) = k1 * x + k2 \mod 26$
- Substitution: $Enc_{perm}(x) = perm(x)$
- Hill cipher, Permutation cipher (not covered in class)

Take a look at the home page for Vigenere/Caesar/etc

Stream Cipher

Keys are short…. Plaintext is long

(P, C, K, L, F, E, D)

P – plaintexts

C – ciphertexts

K – keyspace

L – keystream alphabet

$F = (f_1, ..., f_?)$ keystream generator

$$f_i : K \times P_{i-1} \rightarrow L$$

$\forall z \subset L \ \exists \ e_z \subset E, d_z \subset D$

$$e_z : P \rightarrow C, d_z : C \rightarrow P$$

where $d_z(e_z(x)) = x$

Special cases and examples :

Block cipher :

$z_i = K \ \ \forall z_i \subset L$

Synchronous stream cipher :

f_i is plaintext - independent

⇧

What’s good/bad about it?

Other Historical Ciphers

- Rosetta Stone
- WWII American use of Navajo
- WWII German Enigma machine
- WWII Japanese Purple Machine

D. Kahn. The Codebreakers. Macmillan Co., New York, 1967.

Rosetta Stone

(some material borrowed from Oberlin College)

The key used to decrypt two Egyptian writing systems:

□Hieroglyphs: used for official texts

and

□Demotic: everyday language of the people

Rosetta Stone (contd.)

From 452 to 1822, "Egypt was silent":

The ability to read hieroglyphic inscriptions on monuments and tombs, and papyrus texts using cursive (demotic) scripts, was lost.

However, the spoken language itself survived, … using Greek letters plus 7 signs derived from demotic, as the **Coptic** language.

The problem…

The Rosetta Stone was discovered in July 1799, as Napoleon's troops were demolishing ancient structures to make way for a fort.

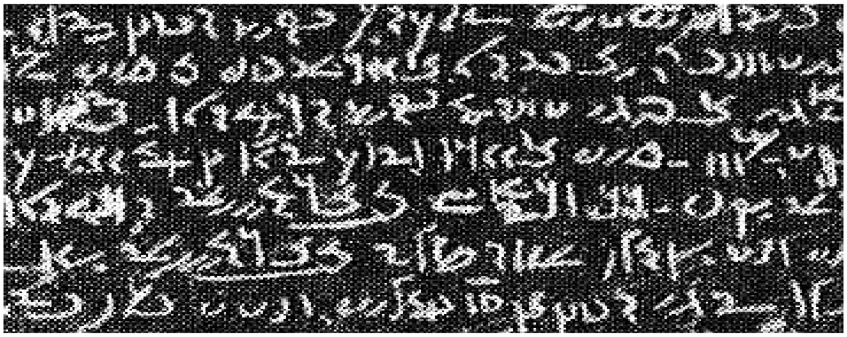
It contains 3 inscriptions, suspected to be a single text in 3 different scripts.

- The first 2 are hieroglyphs and demotic.
- The third inscription is in Greek.

The problem (contd.)

The stone contains 14 lines of hieroglyphs, 32 lines of demotic and 54 lines of Greek.

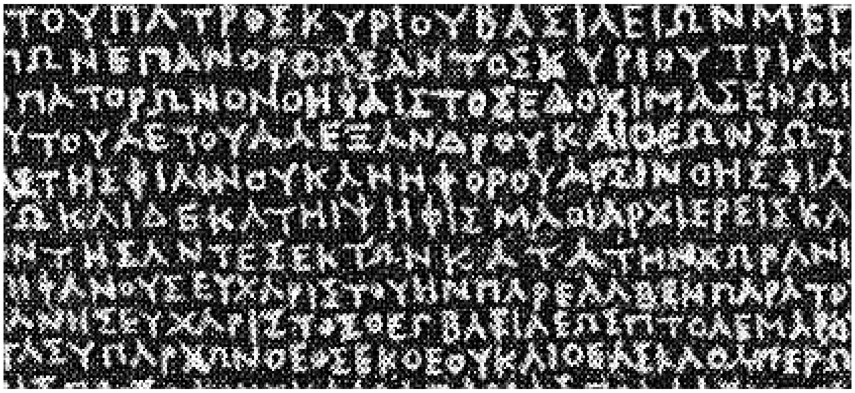
The 14 lines of hieroglyphs are only partial, and correspond to the last 28 lines of Greek, which are also damaged.



The problem (contd.)

The first 14 lines of demotic are damaged at the beginnings.

The last 26 lines of Greek are damaged at the ends.



The solution

Major issue: Are hieroglyphs and demotic texts alphabetic or symbolic?

T. Young showed that both demotic and hieroglyphic writing contain both alphabetic and symbolic elements.

Young's method:

- Find a word in the Greek text which occurred more than once.
- Look for a group of signs in the demotic section which occurred approximately an equal number of times.
- Using this method he was able to identify the demotic for and,which occurred on almost every line.

The solution (contd.)

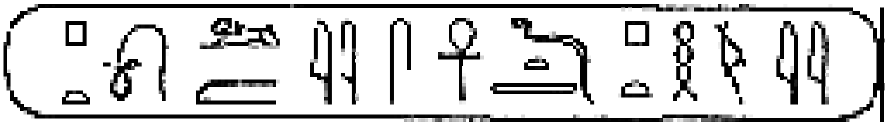
- Words that appeared most frequently were equated with king, Ptolemy (ptolemeus) and Egypt.
- The Greek equivalents were written above the demotic and then he "filled in the gaps".
- This was made more difficult by the fact that the Greek and demotic were not literal translations of each other.

Champollion cracks the code

Despite Young's results, J. F. Champollion believed that hieroglyphs were purely symbolic.

He obtained a copy of a bilingual inscription in hieroglyphs and Greek from the Bankes obelisk.

He (correctly) assumed that the elongated oval (cartouche) contained a royal name.



Bankes' obelisk

William John Bankes, an English traveler, collector and antiquarian, had traveled in Egypt and Nubia and became very interested in the decipherment of Hieroglyphs. A bilingual obelisk from Phila eventually came into the possession of Bankes, was transported to England and set up in his park at Kingston Lacy, Wimborne, where it still stands today.

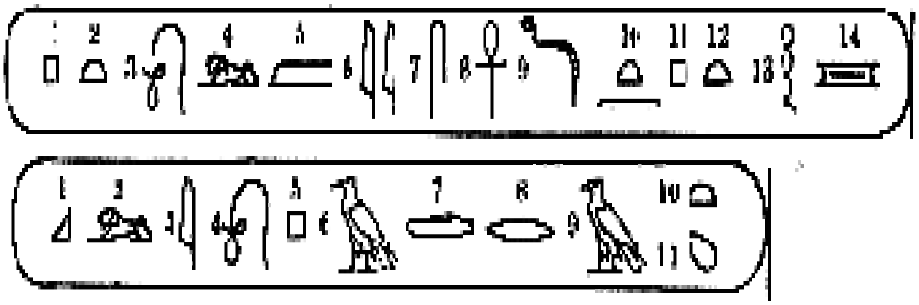
- The only cartouche that appeared 6 times was thought to be Ptolemy, since the Greek section showed that the inscription was about Ptolemy.

- It was also assumed that the characters sound out the Greek form of the name "Ptolemy".

- On the obelisk, the Greek section mentions 2 royal names: Ptolemy and Cleopatra. In the hieroglyphic section two cartouches occurred close together.

- One of them was nearly identical to the cartouche on the Rosetta Stone.

Then the other cartouche from the Bankes obelisk was thought to contain the name of Cleopatra. Now consider Ptolemy and Cleopatra together:



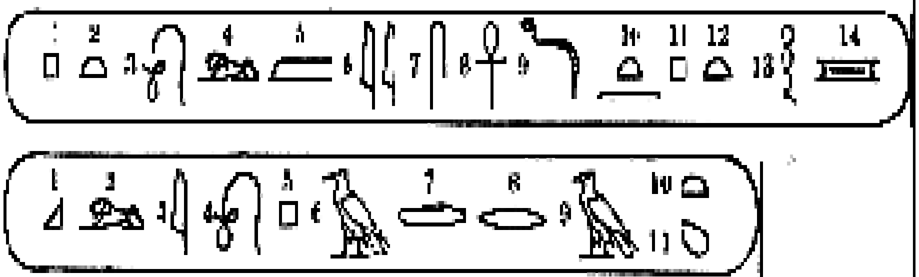
A1 = B5: Must be P.
A4 = B2: Must be L. -------> Then B1 must be K.

Substituting the known letters into Cleopatra:

The 2 vowels E and O between L and P are probably the equivalents of B3 and B4, respectively.

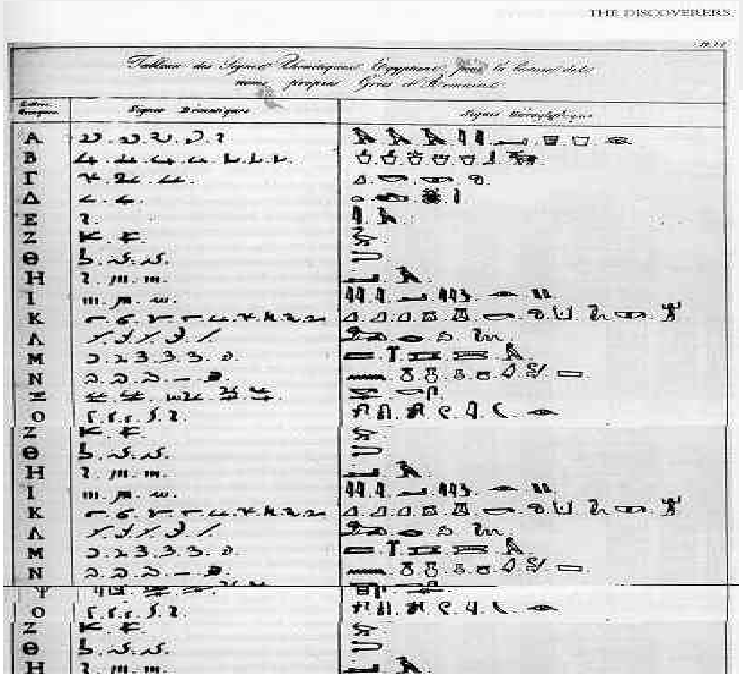
In some forms of the Cleopatra cartouche, B7 is replaced by B10, which is also A2. Both are probably T.

B6 and B9 must be A.



Etc., etc.

T H E K E Y



THE DISCOVERERS

Tableau des Signes Phonétiques Égyptiens pour la lecture des noms propres Grecs et Romains

Lettres Grecques	Signes Démotiques	Signes Hiéroglyphiques
Α		
Β		
Γ		
Δ		
Ε		
Ζ		
Θ		
Η		
Ι		
Κ		
Λ		
Μ		
Ν		
Ξ		
Ο		
Ζ		
Θ		
Η		
Ι		
Κ		
Λ		
Μ		
Ν		
Υ		
Ο		
Ζ		
Θ		
Η		