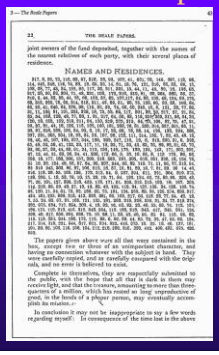
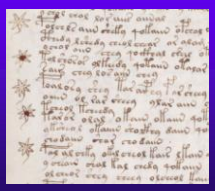
Unbroken Ciphers: Beale



Beale Cipher, 1895

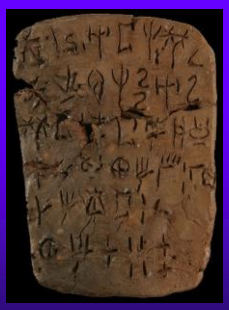
Voynich

Voynich Manuscript, 16th century



See http://beinecke.library.yale.edu/digitallibrary/voynich.html

Linear A

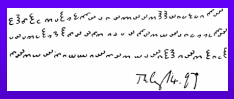


See http://www.archaeology.org/online/reviews/minoans/jpegs/index.php?start=1

RSA Challenges (until 2007)

Unbroken or Unbreakable ?

- Beale Papers
- Dorabella Code
- D'Agapeyeff ciphe
- Kryptos
- Linear A
- Phaistos Disk
- RSA Challenges
- Voynich
- Zodiac Killer



Ciphers or Ciphertexts?

UNBREAKABLE

Baudot Code

Émile Baudot, 1845-1903, French

baud: 1 symbol per second

```
00011     A
11001     B
01110     C
....
01000     CR
00010     LF
```

Teletypewriter

Vernam Cipher I

Gilbert S. Vernam, 1890-1960, American
Invented Vernam cipher in 1918

```
 plaintext  B    A    G
   in code  000111100111010...
       key  0110100110101...
ciphertext  0111011111011...
       key  0110100110101...
      code  000111100111010...
 plaintext  B    A    G
```

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

- like Vigenére with non-repeating key
- is easily implemented using tapes

Vernam Cipher II

```
  plaintext  000111100111010...
        key  0110100110101...
 ciphertext  0111011111011...
```

How to choose key?

- should not repeat key (ever, why?)
- key should be random (no structure)
- long keys are hard to distribute

Vernam Cipher III

Morehouse's solution

- use multiple short tapes ***of different lengths***
- combine results

```
1st tape (3 bits)  010010010010010
2nd tape (5 bits)  110101101011010
               key 100111111001000
```

- Was initially adopted by US army
- open to running-key attacks, as shown by Joseph Mauborgne in 1918

The unbreakable cipher

Mauborgne and Friedman knew that the Vernam cipher is absolutely secure, as long as

- the key is arbitrarily long
- the bits in the key are randomly chosen
- the key is never reused

This cipher is called the **one-time pad**.

Claude Shannon published two papers in 1948 and 1949 which founded the area of information theory.

- allows a definition of perfect security
- can show that one-time pad is perfectly secure