# Cryptography

## 1 Cyphers - from Easy to Hard

Visit www.simonsingh.net/The_Black_Chamber/chamberguide.html to learn and play with different encryption methods:

We will visit the following places in the Black Chamber

- Rail Fence Cypher
- Caesar Cipher
- Kama-sutra Cypher
- Mono-alphabetic Cyphers
- Cracking the Substitution Cyphers
- Letter Frequencies
- Hints and Tips

## 2 Let's Play with Cyphers

Visit http://www.cryptoclub.org/tools/ciphers.php and click Crack Substitution to practice decrypting messages.

Next enjoy the games and stories:

- Click: Games
- Click: Comics

## 3 Public-Key Cryptography

We illustrate public-key cryptography using a "beginner's algorithm". This shows the essential ideas, but you can defeat it if you are clever enough. The actual RSA algorithm uses similar machinery, but no one has been clever enough to defeat it – so far.

The basic requirement is an encryption (coding) operation that depends on a *public key-number* $a$, and which can be decrypted (decoded) using a *private key-number* $b$. Our encryption will be multiplication by the constant $a$ modulo 100, which can be undone by multiplying by the inverse $b = a^{-1}$, meaning the number such that $ba \equiv 1 \pmod{100}$.

**1.** Find a key-number pair by choosing a number $n \equiv 1 \pmod{100}$, factoring it $n = ab$, and reducing the factors mod 100.

EXAMPLE: Sally takes $n = 501 = (3)(167)$. Her key-numbers: $a \equiv 3$, $b \equiv 67 \pmod{100}$.

NOTE: $1 \equiv 501 \pmod{100} = (3)(167) \pmod{100} = 3 \pmod{100} * 167 \pmod{100} = (3)(67) \pmod{100} = 201 \pmod{100} \equiv 1$.

This is because $(3)(167) = (3) * (100 + 67) = 3 * 100 + 3 * 67 \equiv 3 * 67 \pmod{100}$.

Use your own $n = 101, 201, 301, \ldots$ to find your own factors $a, b$ (reduced mod 100).

The smaller factor $a$ will be your *public key*. Write $a$ on the board next to your name, but guard the other factor $b$ with your life: $b$ is your *private key*!

**2a.** Take a one-word message and translate its letters into numbers using the hash table:

| *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 |

**b.** Pick one of the other people to receive your message, and find their public key $a$ on the board. Encrypt by multiplying *your* message-numbers times *their* public key $a$. Write the encrypted message on the board next to the recipient's name.

EXAMPLE: My message for Sally is: `HURRAY`, whose numbers are: 8,21,18,18,1,25. I look up Sally's public key $a = 3$ (but only Sally knows her private key $b$). I encrypt my message by figuring: $8 \times 3 = 24$ , $21 \times 3 = 63$ , $18 \times 3 = 54$ , $1 \times 3 = 3$ , $25 \times 3 = 75$, so next to Sally's name I post: 24,63,54,54,3,75.

**3a.** Find a message for you on the board. Decrypt it by multiplying each number by your private key $b$, then looking up its letter in the table.

EXAMPLE: Sally decrypts my message above by multiplying each number by her private key $b = 67$: $24 \times 67 = 1608 \equiv 8 \pmod{100} =$ `H`; $63 \times 67 = 4221 \equiv 21 \pmod{100} =$ `U`. Eventually, Sally recovers my message `HURRAY`.

**b.** Explain why multiplying by $b$ undoes the encryption (multiplying by $a$).

**4.** Now try to decrypt a message sent to someone else! Letter-frequency analysis is not very useful, since there is not enough text. You need their private key $b$ to decrypt their message, just the way you did with your own message and your own private key.

But all you know is their public key $a$. You need to find $b$ by solving the equation $xa \equiv 1 \pmod{100}$. It is not hard to do!

# 4 The RSA Cryptosystem

**Step 1.** Choose two prime numbers $p$ and $q$ and compute the number

$$n = pq, \quad \text{e.g.} \quad p = 5, q = 11, n = (5)(11) = 55$$

**Step 2.** Choose a number $e$ relatively prime to $(p-1)(q-1)$, e.g.

$$(p-1)(q-1) = (5-1)(11-1) = (4)(10) = 40, \ e = 7$$

**Step 3.** Find decryption number $d$, such that $ed = 1 \pmod{(p-1)(q-1)}$, e.g.

$$ed = 7d = 1 \pmod{(5-1)(11-1)}, \ (7)(23) = 1 \pmod{40}, \ d = 23$$

**Step 4.** Publish your public key

$$(n, e) = (55, 7)$$

ENCRYPTION: Take a message letter **j**, it is the ninth letter in the alphabet so $j = 9$. It will be encrypted as

$$C = 9^e \pmod{n} = 9^7 \pmod{55} = 4.$$

So I send you the number 4. Only you know the decryption number $d = 23$. You can decrypt my message as follows.

$$4^{23} \pmod{55} = 9.$$

How come nobody else can do that? Because all that you published was the number $n = 55$, so nobody knows $p = 5$ and $q = 11$, so nobody can figure our that $ed = 7d \pmod{(5-1)(11-1)} \equiv 1$ to find $d$.

Well, if really $n = 55$ anyone could figure out that $p = 5$, $q = 11$, but in real RSA $p$ and $q$ are huge prime numbers and nobody knows how knowing $n = pq$ one can factor $p$ and $q$ out. Here is an example, say:

$$n = 47141807 = pq$$

can you find $p$ and $q$? Mathematics software can but it crashes if

$$\begin{aligned} n &= 204041065458951029061541285222069954147617165188711659 7 \\ &= 106634041749171059581457216 9 * 191347024000932780814494239 17 \end{aligned}$$

ACTIVITY: Choose you $p$ and $q$ values and publish your public key, keep your decryption number private! Take a one-word message and translate its letters into numbers. Pick one of the other people to receive your message, and find their public key $(n, e)$ on the board. Encrypt using RSA *your* message-numbers using *their* public key $(n, e)$. Write the encrypted message on the board next to the recipient's name. The recipient only can decrypt it using *their* decryption number.

HAPPY ENCRYPTING/DECRYPTING!!!