Cryptography

24-02-2018

Anson Ho
Hello Alice

A$@LSD

Eve

Bob

Origin

Cryptography

Hong Kong Olympiad in Informatics
Cryptography

Application - Military Communication

German soldier A

Alan Turing

Enigma

German soldier B
Application - HTTPS

- **HTTP**
  - Internet
  - MITM

- **HTTPS**
  - Internet

- Man-in-the-middle attack
  - middle = VPN, WiFi router, ...
  - attack = record / modify data
Application - Authentication

Other: zero-knowledge proof
Application - Cryptocurrency

- Block chain
  - decentralization -> P2P
  - Record storage and verification are spread across the network
Application(?) - Cryptoworm

![Image of Wana Decryptor 2.0]

**What Happened to My Computer?**
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**
Sure. We guarantee that you can recover all your files safely and easily. But you have not so much time.

- You can decrypt some of your files for free. Try now by clicking Decrypt.
- But if you want to decrypt all your files, you need to pay.
- You only have 3 days to submit the payment. After that the price will be doubled.
- Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.

We will have free events for users who are so poor that they couldn’t pay in 6 months.

**How Do I Pay?**
Payment is accepted in Bitcoin only. For more information, click About Bitcoin.

- Please check the current price of Bitcoin and buy some bitcoins. For more information, click How to buy bitcoins.
- And send the correct amount to the address specified in this window.
- After your payment, click Check Payment. Best time to check: 9:00am - 11:00am GMT every day to Friday.

Send $300 worth of bitcoin to this address:

126YDFgwueZSNyMgw519p7AA8kj9SSMw

[Check Payment] [Decrypt]
Classical Cipher

● Shift cipher
  ○ Caesar cipher  DEF -> ABC
  ○ ROT13  DEF -> QRS

● Substitution cipher
  ○ DEF -> SWF
  ○ DEF -> PAW

# = 26!
### Classical Cipher

- **Vigenere cipher**\((a + b \mod 26)\)
  - Plaintext: ATTACKATDAWN
  - Key: LEMONLEMONLE \((\text{LEMON})\)
  - Ciphertext: LXFOPVEFRNHR

- **Transposition cipher**
  - ABCDEF -> FEDCBA
  - ABCDEF -> ABC
  - ABCDEF -> FED
Hashing

- OI
  - e.g.: rolling hash
    - will be taught in String Algorithms
  - memory, time <-> a small probability of WA

- General
  - for verification
  - a (hopefully) injective function
    - without collision \((f(a) = f(b) \text{ but } a \neq b)\)
  - easy to compute the value
  - difficult to compute the inverse value
  - usually not “continuous”
    - “a and b are close” does not implies “\(f(a)\) and \(f(b)\) are close”
MD5

- A hashing function
- Software checksum
- No longer safe
- Other:
  - SHA-2
Hashing vs Encryption

- Hashing
  - one-way

- Encryption
  - two-way
  - reverse: decryption
Symmetric / Asymmetric Key Encryption

- **Symmetric Key Encryption**
  - same keys for encryption and decryption
  - e.g. xor
    - 123 xor 456 = 435
    - 435 xor 456 = 123
  - e.g. Advanced Encryption Standard (AES)

- **Asymmetric Key Encryption**
  - different keys for encryption and decryption
    - one public
    - one private
    - two keys are paired, i.e. they cannot be generated independently
RSA

- **Rivest–Shamir–Adleman**

  \[ n = pq \text{ where } p \text{ and } q \text{ are primes} \]

- R.H.S. -> L.H.S. is fast (multiplication)
  - e.g. FFT

- L.H.S. -> R.H.S. is slow (factorization)
RSA

- Euler’s phi function $\phi$
  - will be taught in Mathematics in OI (II)
  - $\phi(pq) = (p - 1)(q - 1)$
  - for fixed $a$, $\phi(n)$ is the length of a cycle of $a^m \mod n$ (not necessary minimum)

- Extended Euclidean algorithm
  - will be taught in Mathematics in OI (I)
  - find G.C.D.
  - find modular inverse

- Fast exponential algorithm
  - a.k.a. big mod algorithm
  - taught in Recursion, Divide and Conquer
RSA

- Preparation
  - find $n = pq$
  - find $de = 1 \pmod{\varphi(n)}$ with $\gcd(e, \varphi(n)) = 1$
  - make the public key $(n, e)$ public
RSA

Encryption

- have plaintext $M$ in mind
  - assume $M$ to be an integer
- get public key $(n, e)$
- calculate $E = M^e \pmod{n}$
- send ciphertext $E$
RSA

● Decryption
  ○ receive ciphertext $E$
  ○ calculate $E^d = (M^e)^d = M \pmod{n}$
    ■ recall that
      ● $de = 1 \pmod{\phi(n)}$
      ● $\phi(n)$ is the length of a cycle of $a^n \pmod{n}$
  ○ retrieve plaintext $M$
### RSA

#### Possible attack
- already know ciphertext $E$ and public key $(n, e)$
- want to know plaintext $M$
  - $E^d = (M^e)^d = M \pmod{n}$
- require private key $d$
  - $de = 1 \pmod{\varphi(n)}$
- require $\varphi(n)$
  - $\varphi(n) = \varphi(pq) = (p - 1)(q - 1)$
- require $p$ and $q$
- need factorization
Cryptography

Attack

- **Brute-force**
  - exhaustion (of keys)
  - look for meaningful outcomes
  - computer performance is increasing incredibly

- **Rainbow table**
  - store all $(x, f(x))$
  - query time ↓
  - memory required ↑
**Attack**

- **Frequency analysis**
  - many $\times$ in ciphertext
  - $\rightarrow$
  - $e$ is possibly replaced by $\times$ during encryption

![Ciphertext Frequency Chart](chart.png)
Cryptography

Attack

● Quantum computing
  ○ Shor algorithm
    ■ polynomial time factorization algorithm
      ● (in terms of number of bits)
    ■ RSA is becoming unsafer
Cryptography

Relation withOI

- Two-step tasks
  - I1123 Parrots
  - M1743 Tree Recovery II
  - S141 Dividing the Cities
  - T144 Lost Sequence

- Huffman coding
  - N1521 荷馬史詩

- Purpose (data compression) sometimes differs from cryptography
IOI01 Double Crypt

\[\text{ciphertext} = E(\text{plaintext}, \text{key})\]
\[\text{plaintext} = E^{-1}(\text{ciphertext}, \text{key})\]

\(E\) and \(E^{-1}\) are given functions (can be called directly).
You may assume their time complexities are \(O(1)\).

**Input:** \(\text{plaintext}, E(E(\text{plaintext}, \text{key1}), \text{key2})\)

**Output:** \(\text{key1}, \text{key2}\)

All items are in 128-bit.

Furthermore, the last 108 bits of the keys are 0.
IOI01 Double Crypt

- Exhaustion of keys
  - $2^{40}$ combinations
  - $2^{40} = 1099511627776$
IOI01 Double Crypt

- Meet in the middle

\[ x = \text{plaintext} \]
\[ y = E(E(\text{plaintext}, \text{key1}), \text{key2}) \]
\[ A_{\text{key1}} = E(x, \text{key1}) \]
\[ B_{\text{key2}} = E^{-1}(y, \text{key2}) \]

- exhaust all A and B
- find the matched pair
CTF

- Capture The Flag

- Computer security competition
  - cryptography
  - reverse engineering
  - pwn
  - etc.

- Allowed to use online resources
For Fun

- Early April Fools?
- Answer: \([A-Z]^*\)
- Answers are somehow meaningful

1. SHOFJEYIWEEETRKJSQUIQHIK
2. 181324542
3. HTEOARRLTIAIZNCODANVL