Crypto/ACM

Phần thi về mã hóa, giải thuật, kỹ năng lập trình…

I love Sherlock Holmes

Posted on 30/05/2014 by Red
Đề bài:

10569512064_f146e4d5d5_b

Không có gì khác, tất cả chỉ vậy thôi, cũng không nói rằng chúng ta phải làm gì.

Đó chính là điều các bạn cần lưu ý, vì trừ trường hợp đặc biệt, còn lại thì chúng ta hiển nhiên cần hiểu rằng mọi bài sẽ có một đòi hỏi duy nhất, đó là tìm ra cờ, và submit kiếm điểm. Thay vì viết là: “Tìm x sao cho: x + 1 = 2″, chúng ta chỉ cần một cái đề: “x + 1 = 2″ cũng đã coi như quá đủ!

Trở lại với công việc, nếu bạn đã từng đọc Holmes (mình thì khỏi nói, mình vô cùng cuồng Holmes và mỗi ngày hầu như đều đọc đi đọc lại mấy mẩu chuyện đã thuộc nằm lòng), thì bạn sẽ nhận ra ngay đây là phương pháp mã hóa xuất hiện trong vụ án “Những hình nhân nhảy múa”, tiếng Anh là Dancing Man. Ở vụ án này, Holmes dựa theo tần suất xuất hiện của từng chữ cái để dần dần suy ra bảng mã tham chiếu hoàn chỉnh. Chúng ta may mắn hơn Holmes, vì chúng ta có Google. Google biết mọi thứ, đó chính là niềm tin của mình.

Search một lúc, ta có bảng mã cho Dancing Man như sau:

Dancing man codes

Đơn giản là đối chiếu đề bài với bảng mã tìm được, chúng ta có dãy ký tự:

RHNTKXTMTEXGMXWWXVMBOX

Nó có phải là cờ không?

Tất nhiên là bạn có quyền thắc mắc như vậy, dù rằng thông thường cờ sẽ không vô nghĩa và xấu xí đến thế.

Khỏi cần thắc mắc dài dòng làm gì, submit thử thì biết chứ có gì đâu.

Wrong!

Đổi sang chữ thường và submit lại.

Wrong!

Đây có lẽ chính là điểm dừng của một số đội chơi khác, vì một lý do quá kinh khủng: không biết phải làm gì nữa

RHNTKXTMTEXGMXWWXVMBOX

Sau khi rà soát lại để chắc chắn rằng không đối chiếu nhầm ở đâu đó, chúng ta sẽ quên hết mọi thứ trong quá khứ, và coi như đề bài chỉ bắt đầu từ cái dòng ký tự xấu xí này mà thôi.

Có khá nhiều hướng khi giải quyết một bài crypto, như XOR các byte với một giá trị x nào đó, cộng thêm một giá trị y nào đó vào từng ký tự, xoay vòng các ký tự theo độ lệch z (cũng nào đó), hoặc phổ biến không kém, đó là hoán vị các ký tự (A thành S, B thành E, C thành X…), và nhiều rất nhiều thuật toán từ cơ bản đến nâng cao khác.

Hướng XOR ít khả thi, do chuỗi ta đang có rất đẹp (đẹp ở đây tức nó đều bao gồm các ký tự chữ cái), mà XOR thì không có đặc tính giữ lại độ đẹp của mật mã sau khi được giải mã (dù rằng một vài giá trị khi dùng làm khóa cũng mang lại điều này). Tuy nhiên, chúng ta vẫn sẽ giữ lại nó trong đầu như một phương án dự phòng.

Cộng thêm giá trị vào các byte, đây là một hướng tốt, có thể thử. Nhưng do mật mã có cả X và B, nên cộng thì cũng dở mà trừ thì cũng dở (vì chắc là nó vượt ra ngoài 2 biên của bảng chữ cái), xếp nó sau XOR theo độ ưu tiên vậy.

Xoay vòng các ký tự (còn gọi là Caesar): Hướng này vô cùng khả thi, do là xoay vòng, nên X + 3 = Z + 1 sẽ quay về A, nên đảm bảo rằng kết quả mã hóa cũng đẹp y như mật mã vậy. Hãy quan tâm đến nó một chút.

Hoán vị các ký tự, hướng này có thể loại ngay, do mật mã quá ngắn, không đủ cơ sở để suy luận.

Caesar

Vấn đề tiếp theo cần đối mặt, đó là nếu chọn Caesar, thì xoay với độ lệch bao nhiêu? Phổ biến thì chúng ta biết đến Rot13 (A sẽ chuyển thành N, B sẽ chuyển thành O, C sẽ chuyển thành P, và ở chiều ngược lại, N sẽ chuyển thành A, O sẽ chuyển thành B, P sẽ chuyển thành C).

Với bài này, Rot13 cho ra kết quả không đẹp:

Rot13(RHNTKXTMTEXGMXWWXVMBOX) = EUAGXKGZGRKTZKJJKIZOBK

Xấu như gấu!

Nhưng Rot13 chỉ là cái người ta hay dùng, và thực tế thì mình đã gặp không ít bài mà người ta Rot16 phút, Rot69, thậm chí Rot linh tinh loạn cả lên. Mà cũng chẳng sao cả, chúng ta có thể dùng một vài tool trên mạng, hoặc tự code vài dòng để có được kết quả của tất cả các phép Rot từ 1 đến 26, và xem xem có kết quả nào khả quan không:

Rot1: SIOULYUNUFYHNYXXYWNCPY
Rot2: TJPVMZVOVGZIOZYYZXODQZ
Rot3: UKQWNAWPWHAJPAZZAYPERA
Rot4: VLRXOBXQXIBKQBAABZQFSB
Rot5: WMSYPCYRYJCLRCBBCARGTC
Rot6: XNTZQDZSZKDMSDCCDBSHUD
Rot7: YOUAREATALENTEDDECTIVE
Rot8: ZPVBSFBUBMFOUFEEFDUJWF
Rot9: AQWCTGCVCNGPVGFFGEVKXG
Rot10: BRXDUHDWDOHQWHGGHFWLYH
Rot11: CSYEVIEXEPIRXIHHIGXMZI
Rot12: DTZFWJFYFQJSYJIIJHYNAJ
Rot13: EUAGXKGZGRKTZKJJKIZOBK
Rot14: FVBHYLHAHSLUALKKLJAPCL
Rot15: GWCIZMIBITMVBMLLMKBQDM
Rot16: HXDJANJCJUNWCNMMNLCREN
Rot17: IYEKBOKDKVOXDONNOMDSFO
Rot18: JZFLCPLELWPYEPOOPNETGP
Rot19: KAGMDQMFMXQZFQPPQOFUHQ
Rot20: LBHNERNGNYRAGRQQRPGVIR
Rot21: MCIOFSOHOZSBHSRRSQHWJS
Rot22: NDJPGTPIPATCITSSTRIXKT
Rot23: OEKQHUQJQBUDJUTTUSJYLU
Rot24: PFLRIVRKRCVEKVUUVTKZMV
Rot25: QGMSJWSLSDWFLWVVWULANW

Nếu tiếng Anh của bạn cũng siêu đẳng như tiếng Anh của mình, bạn sẽ thấy ngay Rot7 là cái mà ta đang tìm, kết quả thu được thực sự quá đẹp:

YOUAREATALENTEDDECTIVE

Nó đẹp đến nỗi mà nó đã có thể là cờ rồi, mình đặt niềm tin với tỉ lệ đặt 6 ăn 9

Wrong!

Wrong!

Wrong!

À hông có sao, còn chữ thường, vẫn còn chữ thường nữa mà

youareatalenteddective

Correct