Bài tập phần mã hoá đối xứng

Câu hỏi 1

Nén dữ liệu thường sử dụng trong lưu trữ và truyền dữ liệu. Giả sử bạn muốn dùng nén dữ liệu kết hợp với mã hóa. Lựa chọn nào dưới đây có có ý nghĩa nhất:

1. Nén sau đó mã hóa.
2. Mã hóa sau đó nén.
3. Thứ tự không quan trọng – không trường hợp nào nén được dữ liệu.
4. Thứ tự không quan trọng – cả hai đều tốt.

Câu hỏi 2

Giả sử bạn biết mã hóa của thông điệp “attack at dawn” dùng one time pad encryption là

```
6c73d5240a948c86981bc294814d
```

(bản rõ ở dạng mã ASCII 8-bit và bản mã được viết ở dạng hexa). Bản mã của thông điệp "attack at dusk"với cùng khóa OTP là gì ?

Câu hỏi 3

Xét (E, D) là một hệ mã an toàn với không gian khóa $K = \{0,1\}^\ell$. Một ngân hàng mong muốn tách khóa giải mã k thuộc $K = \{0,1\}^\ell$ thành hai khóa p_1 và p_2 sao cho để giải mã bắt buộc cần cả hai khóa. Khóa p_1 có thể đưa cho một nhân viên và p_2 cho một nhân viên khác, và cả hai người phải cùng tham gia thì quá trình giải mã mới có thể tiến hành.

Ngân hàng sinh ngẫu nhiên khóa k_1 thuộc $\{0,1\}^\ell$ và đặt $k_1' \leftarrow k \oplus k_1$. Chú ý rằng $k_1 \oplus k_1' = k$. Ngân hàng có thể đưa k_1 cho một nhân viên và k_1' cho nhân viên khác. Cả hai phải có mặt thì quá trình giải mã mới tiến hành được bởi vì bản thân mỗi khóa không chứa thông tin về khóa bí mật k (chú ý rằng mỗi phần là một one-time pad encryption của k).

Bây giờ, giả sử ngân hàng muốn tách k thành ba phần p_1, p_2, p_3 sao cho chỉ cần hai trong số ba khóa là có thể giải mã được. Việc này đảm bảo rằng dù một nhân viên bị ốm thì việc giải mã vẫn có thể tiến hành. Để làm điều này, ngân hàng sinh ngẫu nhiên hai cặp (k_1, k_1') và (k_2, k_2') như trên sao cho $k_1 \oplus k_1' = k_2 \oplus k_2' = k$. Ngân hàng nên gán các phần thế nào để chỉ cần hai phần vẫn có thể giải mã được khóa k, nhưng chỉ có một phần thì không thể ?

1. $p_1 = (k_1, k_2), \quad p_2 = (k_1, k_2), \quad p_3 = (k_2')$
2. $p_1 = (k_1, k_2), \quad p_2 = (k_2, k_2'), \quad p_3 = (k_2')$
3. $p_1 = (k_1, k_2), \quad p_2 = (k_1'), \quad p_3 = (k_2')$
4. $p_1 = (k_1, k_2), \quad p_2 = (k_1', k_2), \quad p_3 = (k_2')$
5. $p_1 = (k_1, k_2), \quad p_2 = (k_1', k_2'), \quad p_3 = (k_2')$

Câu hỏi 4

Ngành công nghiệp phim muốn bảo vệ nội dung số của các đĩa DVD. Chúng ta phát triển một phương pháp để bảo vệ các đĩa Blu-ray gọi là AACS.

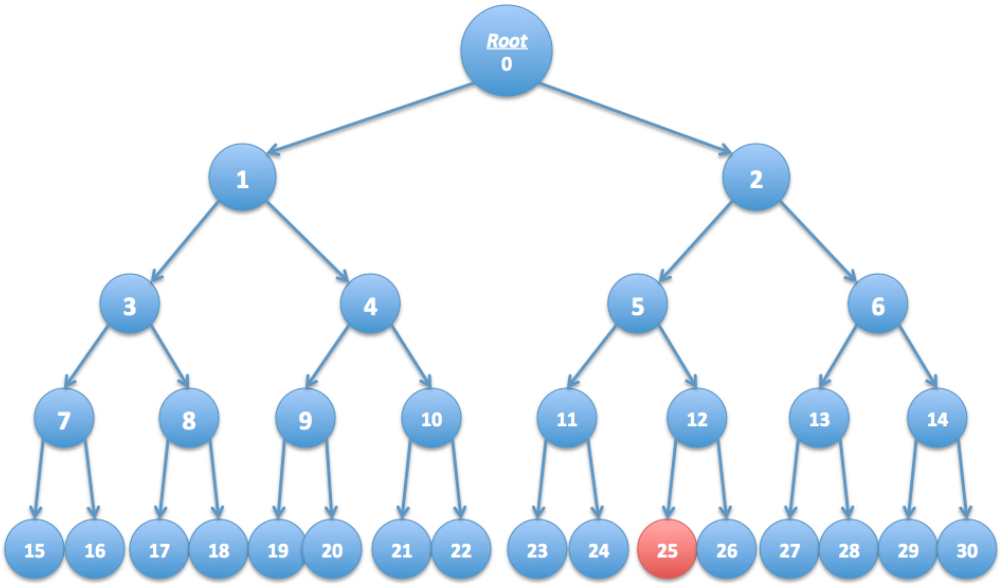
Giả sử tổng số đầu đọc DVD trên thế giới nhiều nhất là n (ví dụ $n = 2^{32}$). Ta xem n đầu đọc như các nút lá của một cây nhị phân có độ cao $\log_2 n$. Mỗi nút trong cây nhị phân này chứa một khóa AES k_i. Các khóa này được giữ bí mật khỏi người dùng và không đổi. Lúc sản xuất, mỗi đầu đọc DVD được gán một số seri $i \in [0, n-1]$. Xét tập các nút S_i dọc theo đường đi từ gốc tới nút lá i trên cây nhị phân. Nhà sản xuất các đầu đọc DVD nhúng trong mỗi đầu đọc có số i một số khóa gắn với nút trong tập S_i. Một đĩa DVD phim m được mã hóa bởi

$$E(k_{\text{root}}, k) \| E(k, m)$$

với k là khóa AES ngẫu nhiên, gọi là khóa nội dụng, và k_{root} là khóa gắn với gốc của cây. Bởi vì mọi đầu đọc DVD đều có khóa k_{root} nên chúng có thể giải mã phim m. Ta gọi $E(k_{\text{root}}, k)$ là header và $E(k, m)$ là body. Dưới đây, mỗi DVD header chứa nhiều bản mã của khóa nội dung k, mỗi bản mã là mã hóa của khóa k dùng khóa k_i trong cây.

Giả sử các khóa được nhúng trong đầu đọc DVD có số r bị lộ do hackers tấn công và bị đưa lên Internet. Mục đích của bài tập này là chỉ ra cách để khi nhà sản xuất phim phân phối một đĩa phim DVD mới, họ có thể mã hóa nội dung của DVD dùng nhiều header hơn một chút (chứa khoảng $\log_2 n$ khóa) sao cho mọi đầu đọc DVD, ngoại trừ đầu đọc có số r, có thể giải mã phim. Thực ra, các hãng sản xuất phim sẽ loại bỏ đầu đọc có số r mà không ảnh hưởng đến các đầu đọc khác.

Như chỉ ra dưới đây, xét cây với $n = 16$ lá. Giả sử nút lá có nhãn 25 tương ứng với đầu đọc DVD có khóa bị lộ. Hãy đánh dấu các khóa dưới đây mà khóa k cần mã hóa sao cho *mọi đầu đọc* khác với đầu đọc 25 có thể giải mã DVD. *Gợi ý:* Chỉ bốn khóa cần mã.



- ☐ 6
- ☐ 1
- ☐ 15
- ☐ 25
- ☐ 11
- ☐ 8
- ☐ 26
- ☐ 16

Câu hỏi 5

Tiếp câu hỏi trước, nếu có n đầu đọc DVD, số khóa cần thiết dùng để mã hóa khóa nội dung k nếu có đúng một đầu đọc DVD cần thu hồi?

- ☐ $\log_2 n$
- ☐ $n-1$
- ☐ $n/2$
- ☐ 2
- ☐ $\sqrt{n}$

Câu hỏi 6

Tiếp câu hỏi 8, giả sử các nút lá gán nhãn 16, 18, and 25 tương ứng với các khóa đầu đọc DVD bị lộ. Đánh dấu tập nhỏ nhất các khóa cần dùng để mã hóa khóa nội dung k sao cho mọi đầu đọc khác các đầu đọc $16, 18, 25$ có thể giải mã DVD. *Gợi ý:* Chỉ cần sáu khóa.

- ☐ 14
- ☐ 15
- ☐ 26
- ☐ 23
- ☐ 4
- ☐ 17
- ☐ 21
- ☐ 0
- ☐ 6
- ☐ 11