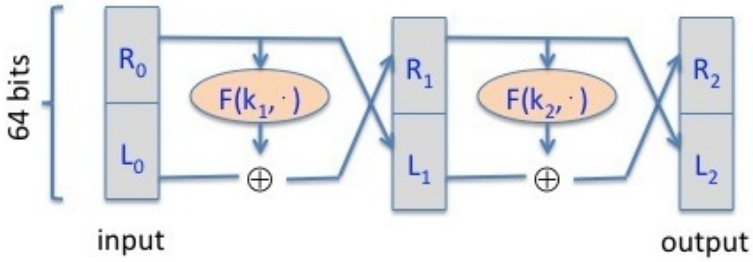
Bài tập 07[1]

Câu hỏi 1

Ta cùng xem chuyện gì xảy ra nếu ta chỉ sử dụng mạng Feistel hai vòng. Xét $F : K \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ là một hàm giả ngẫu nhiên an toàn (PRF). Nhắc lại rằng mạng Feistel 2-vòng được định nghĩa bởi hoán vị ngẫu nhiên (PRP) $F_2 : K^2 \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$. Ở đây R_0 là 32 bits phải của 64-bit đầu vào và L_0 là 32 bit trái.



Một trong các dòng dưới đây là output của PRP F_2 này dùng một khóa ngẫu nhiên, trong khi ba output khác là output của một hoán vị ngẫu nhiên thật $f : \{0,1\}^{64} \rightarrow \{0,1\}^{64}$. Mọi dãy 64-bit outputs đều được mã hóa như các xâu hex độ dài 16. Bạn có thể chỉ ra output của PRP này không? Chú ý rằng, vì bạn có thể phân biệt được ouput của F_2 với ngẫu nhiên, nên F_2 không phải là mã khối an toàn. Đây chính là cái mà chúng ta muốn chỉ ra.

Gợi ý: Đầu tiên ta nên tìm cách nhận biết được mẫu có phải là xor của $F_2(\cdot, 0^{64})$ và $F_2(\cdot, 1^{32}0^{32})$. Sau đó cố gắng nhận biết mẫu này trong output.

1. Với input 0^{64} thì output là "`5f67abaf 5210722b`". Với input $1^{32}0^{32}$ thì output là "`bbe033c0 0bc9330e`".
2. Với input 0^{64} thì output là "`2d1cfa42 c0b1d266`". Với input $1^{32}0^{32}$ thì output là "`eea6e3dd b2146dd0`".
3. Với input 0^{64} thì output là "`e86d2de2 e1387ae9`". Với input $1^{32}0^{32}$ thì output là "`1792d21d b645c008`".
4. Với input 0^{64} thì output là "`4af53267 1351e2e1`". Với input $1^{32}0^{32}$ thì output là "`87a40cfa 8dd39154`".

Câu hỏi 2

Nonce-based CBC. Nhắc lại trong bài giảng rằng nếu muốn dùng mã hóa CBC với nonce không ngẫu nhiên duy nhất thì nonce đầu tiên phải được mã hóa với một khóa PRP độc lập

[1] `https://class.coursera.org/crypto-012/`

và kết quả sau đó được dùng như CBC IV. Ta cùng xem chuyện gì xảy ra nếu ta mã hóa nonce với cùng khóa PRP như khóa dùng cho mã hóa CBC.

Xét $F : K \times \{0,1\}^\ell \to \{0,1\}^\ell$ là một PRP an toàn, ví dụ, $\ell = 128$. Xét n là một nonce và giả sử người ta mã hóa thông điệp m bằng cách: đầu tiên tính $IV = F(k,n)$ và sau đó dùng IV này trong mã hóa CBC dùng $F(k,\cdot)$. Để ý rằng cùng khóa k được dùng cho tính IV và cho mã hóa CBC. Ta chứng minh rằng kết quả là hệ thống không phải là một nonce-based CPA an toàn.

Kẻ tấn công bắt đầu bằng cách hỏi mã hóa của hai khối $m = (0^\ell, 0^\ell)$ với nonce $n = 0^\ell$. Anh ta nhận lại được hai khối bản mã (c_0, c_1). Quan sát rằng, theo định nghĩa của CBC ta biết rằng $c_1 = F(k, c_0)$. Tiếp theo, kẻ tấn công hỏi mã hóa của một khối thông điệp $m_1 = c_0 \bigoplus c_1$ với nonce $n = c_0$. Anh ta nhận lại được một khối bản mã c_0'.

Quan hệ nào dưới đây là đúng với c_0, c_1, c'_0? Để ý rằng quan hệ này giúp kẻ tấn công thắng trong nonce-based CPA game với lợi thế 1.

1. $c_1 = 0^\ell$

2. $c_1 = c_0 \bigoplus c_0'$

3. $c_1 = c_0'$

4. $c_0 = c_1 \bigoplus c_0'$

Câu hỏi 3

Nhắc lại rằng hệ mã không giấu đầy đủ thông tin về độ dài của thông điệp truyền. Lộ thông tin về độ dài của web requests được dùng để nghe trộm thông tin trên traffic HTTPS tới một số trang web, như thông tin chuẩn bị thuế, Google searches, và trang sức khỏe. Giả sử rằng kẻ tấn công nhận được một gói tin mà anh ta biết rằng phần nội dung gói tin được mã hóa dùng AES trong CBC mode với IV ngẫu nhiên. Nội dung gói tin được mã hóa là 128 bytes. Thông điệp nào dưới đây có thể đoán là giải mã của nội dung gói tin:

1. `'The most direct computation would be for the enemy to try all 2^r possible keys, one by one.'`
2. `'If qualified opinions incline to believe in the exponential conjecture, then I think we cannot afford not to make use of it.'`
3. `'We see immediately that one needs little information to begin to break down the process.'`
4. `'In this letter I make some remarks on a general principle relevant to enciphering in general and my machine.'`

Câu hỏi 4

Xét $R := \{0,1\}^4$ và xét PRF $F : R^5 \times R \to R$ được định nghĩa như sau:

$$F(k,x) := \left\{ \begin{array}{l} t = k[0] \\ \text{for } i = 1 \text{ to } 4 \text{ do} \\ \qquad \text{if } (x[i-1] == 1) \quad t = t \oplus k[i] \\ \text{output } t \end{array} \right.$$

Có nghĩa rằng, khóa là $k = (k[0], k[1], k[2], k[3], k[4])$ trong R^5 và giá trị của hàm tại, ví dụ, 0101 được định nghĩa bởi $F(k, 0101) = k[0] \oplus k[2] \oplus k[4]$.

Với một khóa ngẫu nhiên k mà bạn không biết, bạn nhận ra rằng

$$F(k, 0110) = 0011 \quad \text{and} \quad F(k, 0101) = 1010 \quad \text{and} \quad F(k, 1110) = 0110.$$

Giá trị của $F(k, 1101)$ là gì? Để ý rằng vì bạn có thể dự đoán hàm tại một điểm mới, hàm này không phải là PRF an toàn.