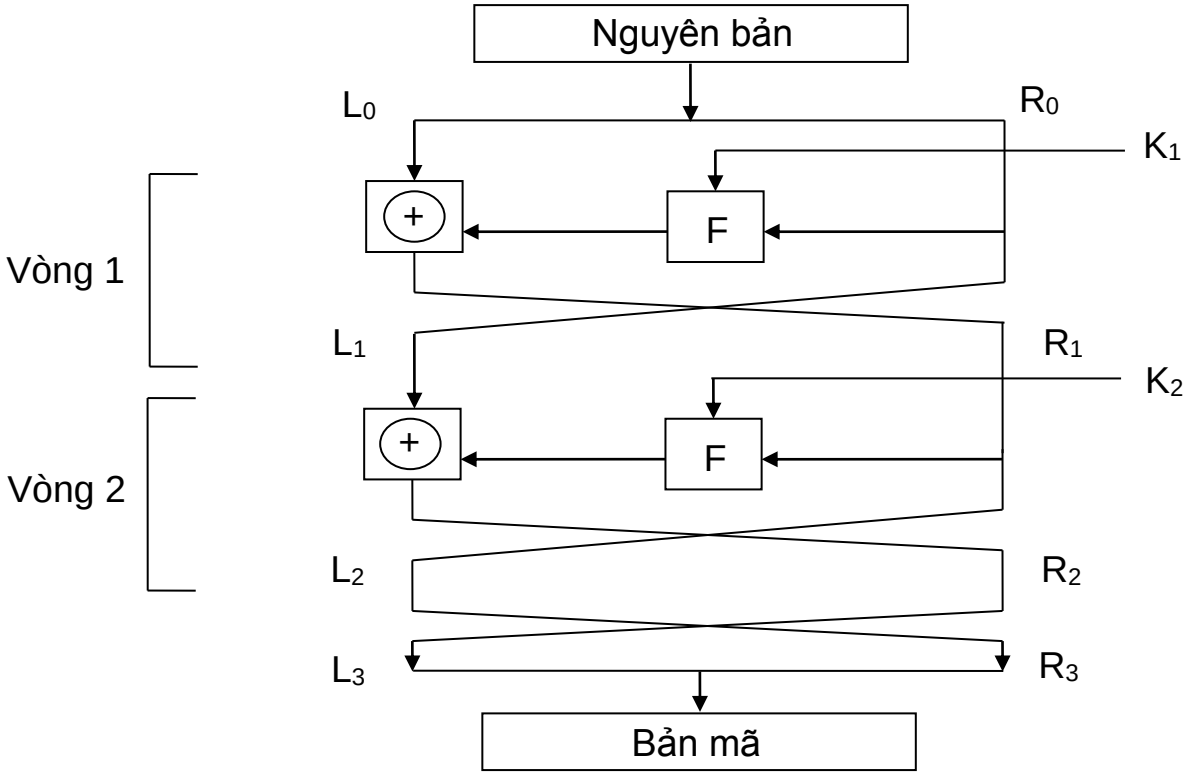
Thời gian : 120 phút
Lớp K47MTT

Được phép tra cứu các loại tài liệu in và photocopy
Cấm sử dụng các giấy viết tay không phải giấy nháp của trường phát

Đáp án đề thi số 1
An toàn Mạng

1. (3 điểm)

Xét một sơ đồ mã hóa Feistel gồm hai vòng như hình vẽ, trong đó hàm vòng F là một hằng số, có nghĩa là tồn tại một chuỗi nhị phân C sao cho F(K, X) = C với mọi K và X.



a. (1 điểm)

Viết công thức tính L_3 và R_3 từ L_0 và R_0 với các khóa con K_1 và K_2.

b. (2 điểm)

Chứng minh rằng một địch thủ không biết giá trị của K_1, K_2 và C vẫn có thể biết được L_0 và R_0 từ L_3 và R_3 bằng hình thức tấn công chọn nguyên bản với chỉ một cặp (nguyên bản, bản mã).

Lời giải

a) Theo sơ đồ ta có

$$L_3 = R_0 \text{ XOR } F(K_2, L_0 \text{ XOR } F(K_1, R_0))$$

$$R_3 = L_0 \text{ XOR } F(K_1, R_0)$$

Vì F(K, X) = C với mọi K và X nên

$L_3 = R_0$ XOR C

$R_3 = L_0$ XOR C

b) Địch thủ có thể thực hiện hình thức tấn công chọn nguyên bản bằng cách yêu cầu giải mã nguyên bản $<L_3, R_3>$, anh ta sẽ thu được bản mã là $<R_3$ XOR C, L_3 XOR C$>$. Ta thấy

$$R_3 \text{ XOR } C = (L_0 \text{ XOR } C) \text{ XOR } C = L_0 \text{ XOR } (C \text{ XOR } C) = L_0 \text{ XOR } 0 = L_0$$

$$L_3 \text{ XOR } C = (R_0 \text{ XOR } C) \text{ XOR } C = R_0 \text{ XOR } (C \text{ XOR } C) = R_0 \text{ XOR } 0 = R_0$$

Vậy bản mã thu được chính là nguyên bản cần tìm.

Bình chú : Câu 1b là trường hợp riêng của một tính chất tổng quát hơn các bạn đã được học trên lớp : Đối với hệ mã hóa Feistel, nếu ta mã hóa một nguyên bản X với các khóa con là $K_1,..., K_n$ (n là số vòng) thu được bản mã Y thì khi giải mã X với các khóa con là $K_n,..., K_1$ ta sẽ thu được nguyên bản chính là Y. Bạn nào nắm vững lý thuyết giảng trên lớp sử dụng tính chất này không cần đả động gì đến phép XOR thì chỉ mất 5' là giải quyết xong toàn bộ câu 1. Tuy nhiên không có bạn nào làm như vậy tức không có ai thật sự vững vàng về lý thuyết toàn sa vào tiểu tiết. Câu 1a mỗi công thức đúng được 0,5 điểm. Một số bạn không viết công thức rút gọn theo đúng đáp án trong câu a nhưng có viết trong câu b thì câu a cũng được tối đa 1 điểm. Câu 1b phần lớn chọn cặp <nguyên bản, bản mã> bất kỳ, tính C, sau đó tính L_0 và R_0. Chọn nguyên bản bất kỳ suy ra bản mã tương ứng được 1 điểm. Viết được công thức tính C được 0,5 điểm. Hoặc chọn nguyên bản là $<L_3, R_3>$ theo như đáp án được 1,5 điểm. Chỉ ra được cách tính L_0 và R_0 từ C và bản mã $<L_3, R_3>$ được 0,5 điểm. Không chỉ ra công thức tính C mà chỉ ra trực tiếp cách tính L_0 và R_0 từ bản mã $<L_3, R_3>$ và cặp <nguyên bản, bản mã> đã chọn cũng được tối đa 2 điểm.

2. (2 điểm)

Xét môđun n trong giải thuật RSA. Như đã biết, thành phần này là một giá trị công khai. Tính xác suất để một số chọn ngẫu nhiên theo phân bố đồng xác suất trong khoảng từ 1 đến $n - 1$ không nguyên tố cùng nhau với n. Nếu tìm được một số như vậy thì hiểm họa gì sẽ xảy ra ? Giải thích.

Lời giải

Trong giải thuật RSA, n là tích của hai số nguyên tố p và q. Số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n theo như đã chứng minh trên lớp

$$\Phi(n) = (p - 1)(q - 1)$$

Như vậy xác suất để một số chọn ngẫu nhiên theo phân bố đồng xác suất trong khoảng từ 1 đến $n - 1$ không nguyên tố cùng nhau với n là

$$1 - \frac{\Phi(n)}{n-1} = 1 - \frac{(p-1)(q-1)}{n-1} = \frac{p+q-2}{n-1}$$

Nếu tìm được một số như vậy thì chỉ việc áp dụng giải thuật Euclid tính ước số chung lớn nhất giữa số vừa tìm thấy và n (là một giá trị công khai).

Ước số chung lớn nhất đó chỉ có thể là p hoặc q. Biết một trong hai số p và q, ta dễ dàng tính được số còn lại và phá mã được hệ RSA đã cho.

Bình chú : Bài này thoạt nhìn thì dễ nhưng bạn nào không nắm vững kiến thức sẽ nghĩ vì n là tích của 2 số nguyên tố nên chỉ có 2 số đó không nguyên tố cùng nhau với n, từ đó suy luận sai là số các số nguyên dương nhỏ hơn n và không nguyên tố cùng nhau với n là 2. Phần tính xác suất và phần chỉ ra hiểm họa chấm độc lập nhau, mỗi phần được tối đa 1 điểm. Chỉ ra công thức đúng tính số các số nguyên tố cùng nhau với n được 0,5 điểm. Chỉ ra công thức đúng tính số các số không nguyên tố cùng nhau với n được 0,75 điểm. Chỉ ra công thức đúng tính xác suất được 1 điểm. Nếu chỉ chỉ ra công thức đúng tính xác suất mà không có suy luận gì thì được 0,25 điểm. Tính sai tử số (tức số các số không nguyên tố cùng nhau với n) nhưng chỉ ra mẫu số (tức số khả năng) đúng là $n - 1$ cũng được 0,25 điểm. Chỉ ra áp dụng giải thuật tính ước số chung lớn nhất được 0,5 điểm. Nói có thể biết p và q được 0,25 điểm. Nói biết p và q suy ra phá mã được được 0,25 điểm.

3. (2 điểm)

Xét một hệ xác thực như sau. Alice lấy một giá trị ngẫu nhiên K làm khóa phiên, rồi gửi định danh ID_A của cô ta và khóa K cho Bob, tất cả những thông tin này được mã hóa sử dụng khóa công khai KUB của Bob. Bob gửi lại cho Alice định danh ID_B của anh ta cùng với khóa K cho Alice, tất cả được mã hóa sử dụng khóa công khai KUA của Alice.

$$\text{Alice} \rightarrow \text{Bob}: \quad E_{KUB}[ID_A \,||\, K]$$

$$\text{Bob} \rightarrow \text{Alice}: \quad E_{KUA}[ID_B \,||\, K]$$

Một địch thủ tên Eve có khả năng chặn được các thông báo Alice và Bob gửi cho nhau cũng như gửi được thông báo cho Alice và Bob.

a. (1 điểm)

Theo giao thức trên đây, Eve có thể giả mạo Alice, tức là có thể làm cho Bob tin rằng Eve chính là Alice được không ? Giải thích.

b. (1 điểm)

Eve có thể giả mạo Bob, tức là có thể làm cho Alice tin rằng Eve chính là Bob được không ? Giải thích.

Lời giải

a) Eve có thể giả mạo Alice khi giao tiếp với Bob bằng cách tự sinh ra một giá trị ngẫu nhiên K, ghép nó với ID_A, mã hóa tất cả bằng khóa công khai KUB của Bob rồi gửi bản mã cho Bob. Bob nhận được thông báo của Eve, nhìn thấy ID_A sẽ nghĩ là đang nói chuyện với Alice, Bob không thể biết được giá trị ngẫu nhiên K là do Eve sinh ra chứ không phải Alice sinh ra. Sau đó Eve và Bob có thể trao đổi với nhau sử dụng khóa K của Eve để mã hóa các thông báo theo phương pháp mật mã đối xứng mà Bob không hề hay biết gì, cứ nghĩ là trao đổi với Alice.

Cách khác : Ngay cả khi không biết ID_A, Eve vẫn có thể giả mạo được Alice khi giao tiếp với Bob bằng hình thức tấn công lặp lại. Cô ta chỉ việc ghi lại một thông báo Alice gửi cho Bob trong quá khứ, sau đó gửi lại cho Bob. Tuy nhiên trong trường hợp này Eve không thể biết được giá trị khóa K vì không có khóa riêng của Bob để giải mã bản mã $E_{KUB}[ID_A \,||\, K]$.

b) Eve không thể giả mạo được Bob khi giao tiếp với Alice. Vì giá trị ngẫu nhiên *K* là do Alice sinh ra. Giá trị này được mã hóa với khóa công khai của Bob. Eve không có khóa riêng của Bob nên không thể giải mã bản mã Alice gửi cho Bob để lấy ra giá trị *K*. Không biết *K*, Eve không thể gửi được cho Alice bản mã có chứa *K* để giả mạo Bob. Lưu ý là ID_A tất nhiên phải khác ID_B nên Eve không thể lấy nguyên bản mã Alice gửi cho Bob để gửi lại cho Alice.

Bình chú : Với mỗi câu chỉ cần nêu đáp án đúng là được 0,5 điểm. Giải thích đúng được thêm 0,5 điểm. Một số bạn không nắm vững khái niệm độ an toàn nên làm sai câu b vì vận dụng sai một bài tập trong các đề thi thử. Bài tập đó yêu cầu phân tích độ an toàn của 3 phương án thực hiện xác thực. Trong thực tế 3 phương án đó đều an toàn vì xác suất tấn công thành công là nhỏ, nhưng phương án nào chi phí tấn công lớn hơn thì được coi là an toàn hơn. Giống như một hệ mã hóa dùng khóa có độ dài 1024 bit thì an toàn hơn là một hệ mã hóa dùng khóa có độ dài 512 bit vì chi phí phá khóa 1024 bit lớn hơn chi phí phá khóa 512 bit. Hai hệ này về lý thuyết đều có thể phá mã được bằng phương pháp vét cạn, tuy nhiên trong thực tế đều được coi là an toàn vì chi phí bỏ ra đều rất lớn. Với câu b, Eve có thể lưu lại rất nhiều thông báo Alice gửi cho Bob và thông báo tương ứng Bob trả lời Alice để đến khi nào Alice gửi cho Bob một thông báo trùng với một thông báo Eve đã lưu sẵn thì Eve trả lời Alice thông báo tương ứng thay cho Bob để giả mạo Bob. Tuy nhiên xác suất để một giá trị ngẫu nhiên *K* do Alice chọn trùng với một số ngẫu nhiên trước đó là rất nhỏ nên có thể coi là Eve không thể giả mạo được Bob. Chẳng hạn, nếu giá trị ngẫu nhiên có độ dài 128 bit, và tốc độ Alice gửi thông báo cho Bob là 10^6 thông báo / μs thì Eve cần chờ $5{,}4.10^{18}$ năm mới có thể nhận được một thông báo trùng với một thông báo lưu trước. Với các ứng dụng an toàn mạng thì giả thiết ngầm định là độ dài khóa, độ dài số ngẫu nhiên được chọn đủ lớn để không thể phá mã bằng phương pháp vét cạn. Tất cả những điều này đã được giảng trên lớp, thế nên bạn nào làm sai nhiều khả năng là do lười đi học, ôn tập không tốt, chỉ học tủ những đề thi thử. Bạn nào trả lời sai câu b nhưng có nêu lên ý khó khăn, phức tạp, tốn nhiều thời gian thì được tối đa 0,5 điểm. Hoàn toàn không nhắc tới ý đó thì được 0 điểm. Có nhắc tới ý nếu miền giá trị của số ngẫu nhiên lớn thì không thể giả mạo được cũng được tối đa 1 điểm. Lưu ý trong câu a, Eve gửi lại một thông báo cũ của Alice cho Bob, Bob nghĩ là Alice gửi một thông báo mới trong khi thực sự tại thời điểm đó Alice không gửi gì cho Bob cả. Bob không phát hiện ra điều này. Thế nên Eve được coi là giả mạo thành công Alice. Trong khi nếu Eve chỉ chặn thông báo Alice đang gửi cho Bob rồi gửi tiếp ngay cho Bob thì không được coi là giả mạo vì đúng là Alice muốn gửi cho Bob thông báo đó thật, Bob tin vào một sự thật đúng, chứ không phải tin vào một sự thật sai. Bạn nào không nói rõ Eve lấy một thông báo cũ Alice gửi cho Bob để gửi cho Bob thì bị trừ 0,5 điểm. Tương tự như vậy, một số bạn nói Eve chặn thông báo Bob đang gửi trả lời cho Alice để gửi tiếp cho Alice, như thế giả mạo được Bob. Điều này là sai và không được điểm nào. Eve chỉ giả mạo được Bob khi tại thời điểm đó Bob không gửi gì cho Alice hoặc có gửi nhưng nội dung thông báo khác với thông báo Bob gửi mà Alice không phát hiện ra.

4. (3 điểm)

Xét một hệ xác thực dựa trên mật mã đối xứng sử dụng một server xác thực S hoàn toàn đáng tin cậy. Hai bên A và B không có khóa bí mật chung cho trước. Nếu muốn truyền thông tin mã hóa cho nhau thì A và B cần xác thực lẫn nhau thông qua S và xin S phân

phối khóa phiên dùng chung. Server S biết khóa bí mật *KA* của A và khóa bí mật *KB* của B. A và B không cho ai biết các khóa *KA* và *KB* tương ứng ngoài S. Giao thức xác thực hai chiều và phân phối khóa tiến hành theo các bước sau :

(1) $A \rightarrow B$: $T \,||\, ID_A \,||\, ID_B \,||\, E_{KA}[RA \,||\, T \,||\, ID_A \,||\, ID_B]$

(2) $B \rightarrow S$: $T \,||\, ID_A \,||\, ID_B \,||\, E_{KA}[RA \,||\, T \,||\, ID_A \,||\, ID_B] \,||\, E_{KB}[RB \,||\, T \,||\, ID_A \,||\, ID_B]$

(3) $S \rightarrow B$: $T \,||\, E_{KA}[RA \,||\, K] \,||\, E_{KB}[RB \,||\, K]$

(4) $B \rightarrow A$: ???

Trong đó, T là nhãn thời gian của A tại thời điểm A thực hiện bước (1) của giao thức, ID_A là định danh của A, ID_B là định danh của B, *RA* là một số ngẫu nhiên tạo ra bởi A tại thời điểm A thực hiện bước (1), *RB* là một số ngẫu nhiên tạo ra bởi B tại thời điểm B thực hiện bước (2), *K* là khóa phiên chọn bởi S tại thời điểm S thực hiện bước (3).

Giao thức cho phép A và B cùng nhận được khóa bí mật chung *K*. Hơn nữa A và B đều biết chắc chắn rằng chỉ A và B biết được *K*.

a. (1 điểm)

Viết thông báo B gửi cho A ở bước (4) của giao thức.

b. (1 điểm)

Giải thích tại sao A và B biết được chắc chắn chỉ họ mới biết giá trị của *K*.

c. (1 điểm)

Giải thích vai trò của *T*, *RA* và *RB*.

Lời giải

a) Thông báo B gửi cho A ở bước (4) của giao thức là

$$T \,||\, E_{KA}[RA \,||\, K]$$

Suy luận (đề bài không yêu cầu nêu rõ suy luận chỉ cần viết công thức) : Mục đích của hệ đã cho là phân phối khóa phiên *K* từ S đến A và B. B nhận được *K* ở bước (3) khi giải mã $E_{KB}[RB \,||\, K]$. A phải nhận được *K* ở bước (4). B nhận được $E_{KA}[RA \,||\, K]$ ở bước (3) nhưng không biết khóa *KA* nên không thể giải mã được bản mã này. Như vậy, B phải hiểu là thông báo $E_{KA}[RA \,||\, K]$ không dành cho anh ta, mà chính là S muốn anh ta chuyển nó cho A. A nhận được $E_{KA}[RA \,||\, K]$ sẽ dùng khóa *KA* của anh ta để giải mã lấy ra khóa phiên *K*. Tóm lại thông báo B gửi cho A ở bước (4) phải chứa ít nhất thành phần $E_{KA}[RA \,||\, K]$.

T đánh dấu thời điểm A khởi tạo một phiên phân phối khóa (bước (1)). Trong khi chờ S phân phối khóa dùng chung với B, A có thể đồng thời xin S phân phối khóa dùng chung với một đối tác khác B. Ngược lại, B cũng có thể đang tiến hành một phiên phân phối khóa với một đối tác khác A. Thế nên phải phân biệt các phiên phân phối khóa bằng nhãn thời gian. Mỗi phiên phân phối khóa có một nhãn thời gian *T* duy nhất. Giá trị ngẫu nhiên sinh tại các thời điểm khác nhau (có nhãn thời gian *T* khác nhau) thì nói chung là khác nhau. Từ nhãn thời gian *T* thì ở bước (3), B mới tra ra được giá trị *RA* tương ứng sinh ra ở bước (1). Tương tự như vậy, ở bước (4), A phải biết nhãn thời gian *T* mới có thể tra ra *RA* tương ứng để kiểm tra tính toàn vẹn của bản mã $E_{KA}[RA \,||\, K]$. *T* trong thông báo ở các bước (1) và (2) phải được mã hóa để đảm bảo tính toàn vẹn vì khi đó B và S chưa biết *T*.

Trong khi ở bước (3) *T* không cần mã hóa vì nếu *T* bị thay đổi thì B sẽ tra ra *RB* tương ứng không khớp với *RB* trong $E_{KB}[RB \| K]$ và B phát hiện ra ngay. Tương tự như vậy, ở bước (4), *T* không cần mã hóa vì nếu *T* bị thay đổi thì A sẽ tra ra *RA* tương ứng không khớp với *RA* trong $E_{KA}[RA \| K]$.

b) Ở bước (3) B giải mã $E_{KB}[RB \| K]$ thu được *RB* và *K*, B đối chiếu *RB* này với *RB* sinh ra ở bước (2), thấy trùng khớp, có nghĩa *RB* và *K* còn toàn vẹn không bị sửa đổi. Vì ngoài *B* chỉ có S là biết *KB*, nên B yên tâm là *K* do S gửi chứ không phải một bên nào khác gửi. B biết là bản mã $E_{KA}[RA \| K]$ do B gửi cho A ở bước (4) chỉ có A giải mã được, bất kỳ địch thủ nào ở giữa dù có bắt được bản mã này đi chăng nữa thì do không có khóa *KA* nên không thể biết được giá trị *K* bên trong. Vậy B biết ngoài A và chính anh ta không có ai biết được giá trị của *K* (tất nhiên có S cũng biết *K* nhưng vai trò của server S là đặc biệt không tính đến ở đây, "không ai khác" ngầm hiểu là "không ai khác trong số các client").

A khi nhận được $E_{KA}[RA \| K]$ ở bước (4) giải mã thu được *RA* và *K*, B đối chiếu *RA* này với *RA* sinh ra ở bước (1), thấy trùng khớp, có nghĩa là *RA* và *K* còn toàn vẹn không bị sửa đổi. Vì ngoài A chỉ có S biết *KA* nên A yên tâm là *K* do S tạo ra chứ không phải của một bên nào khác. A thấy B gửi cho mình $E_{KA}[RA \| K]$ hợp lệ, mà bản mã này B không tự tạo ra được nên A biết là B đã nhận được nó từ S. A đối chiếu giao thức thấy khi S gửi cho B $E_{KA}[RA \| K]$ thì cũng gửi cho B $E_{KB}[RB \| K]$. A hoàn toàn tin tưởng vào S nên biết chắc chắn là B nhận được $E_{KB}[RB \| K]$ chứ không khi nào S lại quên gửi cho B bản mã này. A biết chỉ B có *KB* nên chỉ B giải mã lấy ra được *K*. Vậy A biết ngoài B và chính anh ta không có ai biết được giá trị của *K*.

c) *T* dùng để phân biệt các phiên xác thực khác nhau và tránh hình thức tấn công lặp lại. *RA* và *RB* dùng để kiểm tra tính xác thực của *K* (toàn vẹn, hợp thời gian, và đúng là phát sinh từ S). Xem thêm giải thích ở trên.

Bình chú : Câu a chỉ cần chứa hai thông tin tối thiểu theo như đáp án là được tối đa 1 điểm. Thiếu mỗi thông tin trừ đi 0,5 điểm. Thừa thông tin nói chung không bị trừ điểm. Tuy nhiên nếu thừa những thông tin vô lý A không thể đọc được như $E_{KB}[...]$ thì bị trừ 0,25 điểm. Giao thức trong đề bài là giao thức Otway-Rees gốc với những thông tin tối thiểu ở bước (4) (xem tệp pdf đính kém), nhưng sau đó có những cải tiến với nhiều thông tin hơn để đảm bảo an toàn hơn (chẳng hạn tham khảo bài báo của Wang và Qing ở địa chỉ http://www.i2r.a-star.edu.sg/icsd/staff/guilin/papers/SEC00-137-fl.pdf). Câu b nếu chỉ nói A biết *K*, B biết *K* mà không giải thích *K* mà A nhận được trùng với *K* mà B nhận được thì chỉ được 0,5 điểm. Phải nói thêm ý A biết *K* nhận được là do S sinh ra, B biết *K* nhận được cũng là do S sinh ra, A và B tin S sinh cùng giá trị *K* cho A và B. Như vậy mới được tối đa 1 điểm. Hầu hết các bạn tập trung nhắc tới tính bảo mật của *K* (tức ngoài A, B và S, không có ai khác biết *K*) mà quên đi tính xác thực (tức A và B khi giải mã được *K* biết chỉ có thể do S tạo ra). Nhắc tới ý A và B biết *K* do S sinh ra, nhưng không nói A và B tin S sinh ra cùng giá trị *K* thì được thêm 0,25 điểm. Câu c giải thích đúng vai trò của *T* được 0,5 điểm. Giải thích đúng vai trò của *RA* và *RB* được 0,5 điểm. Nếu chỉ nói *T* dùng để tránh hình thức tấn công lặp lại không nêu lên ý để phân biệt các phiên xác thực (và phân phối khóa) thì chỉ được 0,25 điểm. Nếu chỉ nói chung chung tác dụng của RA và RB là để kiểm tra tính xác thực của *K*, không giải thích rõ kiểm tra như thế nào thì chỉ được 0,25 điểm. Nếu không nói rõ cách thức kiểm tra trong câu c nhưng đã nói ở câu b thì vẫn được 0,5 điểm.

Phương án chấm điểm phòng 402

Đối với phòng 207+307

+ 44/44 bài được 1 điểm cho câu 1a

+ 1/44 bài được 0 điểm cho câu 1b. Bài này cá biệt chỉ được tổng cộng 2 điểm, 1 điểm cho câu 1a và 1 điểm cho câu 1b. Còn 43 bài còn lại đều có ít nhất 1 điểm cho câu 1b.

==> Đối với phòng 402, những ai làm được câu 1a sẽ được 2 điểm thay vì 1 điểm.

* Thực tế chấm phòng 402, có 21/22 bài được 2 điểm cho câu 1a, chỉ một bài được 1,5 điểm.

Đối với phòng 207+307

+ 43/44 bài trả lời đúng câu 3a là Eve có thể giả mạo được Alice và được 0,5 điểm cho phần này. Trong đó có 41 người được 1,5 điểm trở lên cho câu 1b.

==> Đối với phòng 402, những ai trả lời đúng ý câu 3a là Eve có thể giả mạo được Alice thì được 1 điểm thay vì 0,5 điểm (phần giải thích vẫn chấm theo thang điểm 0,5).

* Thực tế chấm phòng 402, có 20/22 bài được 1 điểm vì trả lời đúng Eve có thể giả mạo được Alice cho câu 3a. Có 2/22 bài được 0 điểm vì trả lời sai ý này, nhưng đều được tối đa 1,5 điểm cho câu 4a (xem cách chấm ở dưới), và tổng điểm là 4,75 và 5,5 nên nếu được cộng thêm 0,5 điểm thì kết quả cuối cùng không thay đổi.

Đối với phòng 207+307

+ 33/44 bài được 1 điểm cho câu 4a

+ 36/44 bài được 2 điểm cho câu 1b

==> Đối với phòng 402, điểm câu 4a tăng từ 1 điểm lên 1,5 điểm.

+ 8/44 bài được 0,75 điểm cho câu 4a và 2 điểm cho câu 1b

+ 1/44 bài được 0,75 điểm cho câu 4a và 1,5 điểm cho câu 1b

+ 1/44 bài được 0,75 điểm cho câu 4a và 1 điểm cho câu 1b

+ 4/44 bài được 1 điểm cho câu 4a và 1,5 điểm cho câu 1b

+ 1/44 bài được 1 điểm cho câu 4a và 1 điểm cho câu 1b

==> Đối với phòng 402, nếu câu 4a bị trừ 0,25 điểm thì trừ đi 0,5 điểm. Nhưng nếu có suy luận có lý ở câu 1b sẽ chỉ bị trừ 0,25 điểm.

* Thực tế chấm phòng 402, có 20/22 bài được 1,5 điểm cho câu 4a. Có 2/22 bài chỉ được 1 điểm, nhưng đều được tối đa 1 điểm vì trả lời đúng ý Eve có thể giả mạo được Alice cho câu 3a (xem cách chấm ở trên), và tổng điểm là 5 và 5,5 nên nếu được cộng thêm 0,25 điểm (trừ 0,25 và cộng thêm 0,5) thì kết quả cuối cùng không thay đổi.