|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Trang** | **Lỗi** | **Sửa lỗi** |
| 1 | 55 | Biểu diễn lũy thừa, tập hợp các phần tử |  |
| 2 | 95 | UTMS | UMTS |
| 3 | 99 | Hoạt động của tầng này được miêu tả bởi hàm sau: | Hoạt động của lớp này được miêu tả bởi hàm sau: |
| 4 | 100 | Hàm *S*() là một 32x32 nhận… | Hàm *S*() là một 32x32 S-box nhận… |
| 5 | 105 | 128-EEA3 dùng để mã hóa và giải mã dữ liệu có độ dài từ 1 đến 2000 bit | 128-EEA3 dùng để mã hóa và giải mã dữ liệu với các khối (block) có độ dài từ 1 đến 20000 bit |
| ? | 105 | COUNT, BEARER, DIRECTION là các tham số dùng để thiết lập generator. Giá trị của các biến này sẽ được gửi kèm cùng với bản mã? | COUNT, BEARER, DIRECTION là các tham số dùng để thiết lập generator. Bộ ba biến này kết hợp lại tạo thành biến nonce cho quá trình mã hóa, giải mã và được đính kèm vào bản mã. |
| 6 | 106 | IV12 = IV4 | IV12 = IV4 |
| 7 | 12 | Hình 1. Logo 3GPP | Hình 1. Logo của tổ chức 3GPP |
| 8 |  | [Lặp chữ “ngày nay”,”tiện dụng cho người dùng”,”quan tâm” XHuy đã sửa lại chút vì Xhuy thấy như vậy sẽ mượt hơn]  Ngày nay, với sự phát triển vượt bật của công nghệ thông tin và truyền thông, đã đem lại rất nhiều những ứng dụng tiện dụng đến với người dùng. Xu hướng phát triển của công nghệ ngày nay là trên môi trường mạng, trong đó mạng di động đang và sẽ có nhiều hứa hẹn đem đến rất nhiều tiện dụng cho người dùng. Trong tương lai gần như mọi ứng dụng đều có thể đưa lên chiếc điện thoại gọn nhẹ. Vấn đề bảo mật ngày nay không chỉ cấp bách trong mạng internet toàn cầu, mà ngay cả ở mạng di động cũng rất cần được sự quan tâm. Nhu cầu đảm bảo bí mật khi thực hiện các cuộc gọi, hay các dịch vụ thông qua mạng di động là điều mà người dùng rất quan tâm. Điều này càng được quan tâm hơn khi có sự xuất hiện thêm hàng loạt những công nghệ mạng di động mới như GPRS, 3G, EPS (LTE – SAE), …. Các công nghệ này đều do tổ chức 3GPP công bố. Dưới đây là Logo của tổ chức 3GPP, được lấy từ trang web của tổ chức (<http://www.3gpp.org/>) | Ngày nay sự phát triển vượt bật của công nghệ thông tin và truyền thông đã đem lại rất nhiều những ứng dụng tiện dụng đến với người dùng. Xu hướng của công nghệ hiện đại là tập trung phát triển trên môi trường mạng, trong đó mạng di động đang và sẽ có rất nhiều hứa hẹn. Trong tương lai gần như mọi ứng dụng đều có thể đưa vào một chiếc điện thoại gọn nhẹ. Vì vậy vấn đề bảo mật ngày nay không chỉ cấp bách trong mạng internet toàn cầu, mà ngay cả ở mạng di động cũng rất cần được sự quan tâm. Nhu cầu đảm bảo bí mật khi thực hiện các cuộc gọi, hay các dịch vụ thông qua mạng di động là điều mà người dùng rất quan tâm, nhất là ngày càng xuất hiện thêm hàng loạt những công nghệ mạng di động mới như GPRS, 3G, EPS (LTE – SAE), …. Các công nghệ này đều do tổ chức 3GPP công bố. Ảnh dưới đây là Logo của tổ chức 3GPP, được lấy từ trang web của tổ chức (<http://www.3gpp.org/>) |
| 9 | 12 | [lặp chữ được ]  Để đáp ứng được các nhu cầu bảo mật trên mạng di động, các công nghệ di động được nói trên đều áp dụng các kỹ thuật mã hóa phù hợp. | Để đáp ứng các nhu cầu bảo mật trên mạng di động thì các công nghệ di động đều phải áp dụng các kỹ thuật mã hóa phù hợp. |
| 9 | 13 | [cụm từ “như ta đã biết ” không cần thiết  ]  Trong đó như ta đã biết, mã khối sẽ làm việc bằng cách chia khối dữ liệu cần mã hóa ban đầu thành những khối dữ liệu nhất định | Trong đó, mã khối sẽ làm việc bằng cách chia khối dữ liệu cần mã hóa ban đầu thành những khối dữ liệu nhất định |
| 10 | 13 | Trên công nghệ Wi-Fi, ở phiên bản 802.11a/b còn đang sử dụng mã dòng RC4, nhưng sang phiên bản 802.11i thì được thay thế bởi mã khối AES | Trên công nghệ Wi-Fi, ở phiên bản IEEE 802.11a/b còn đang sử dụng mã dòng RC4, nhưng sang phiên bản IEEE 802.11i thì được thay thế bởi mã khối AES |
| 11 | 13 | [Lặp chữ “vào thời gian đó”]  Vào thời gian đó, rất nhiều tổ chức sử dụng đến mã dòng như: những nhu cầu của quân đội và ngoại giao, các tổ chức gián điệp, các tổ chức cung cấp dịch vụ viễn thông, các doanh nghiệp,… Vào thời gian đó những thiết bị mã hóa điện tử bán dẫn đã bắt đầu xuất hiện. Nhiều thiết bị còn có bộ nhớ với dung lượng rất thấp, nên mã dòng trở nên phổ biến hơn mã khối | Vào thời gian đó, rất nhiều tổ chức sử dụng đến mã dòng như: những nhu cầu của quân đội và ngoại giao, các tổ chức gián điệp, các tổ chức cung cấp dịch vụ viễn thông, các doanh nghiệp,… Những thiết bị mã hóa điện tử bán dẫn cũng đã bắt đầu xuất hiện. Do các thiết bị này có dung lượng bộ nhớ thấp nên mã dòng trở nên phổ biến hơn mã khối. |
| 12 | 13 | Nhưng không vì vậy mà mã dòng lại không thể phát triển được. Hội thảo ***The State of the Art of Stream Ciphers***, một hội thảo chuyên về mã dòng, vẫn đang được thu hút. | <nên thêm thời gian và địa điểm> |
| 13 | 17 | **Phụ lục A** trình bày một số đặc tính mật mã khác của hàm Boolean và của S-box ảnh hướng đến tính an toàn của bộ sinh là: bậc đại số (algebraic degree) và độ miễn đại số (algebraic immunity). | **Phụ lục A** trình bày một số đặc tính mật mã khác của hàm Boolean và của S-box ảnh hướng đến tính an toàn của bộ sinh là bậc đại số (algebraic degree) và độ miễn đại số (algebraic immunity). |
| 14 | 20 | **Đối với mã khối**, khi mã hóa, dữ liệu ban đầu được chia thành các khối (block) thường thì có kích thước bằng nhau, và kích thước này sẽ tùy thuộc vào thuật toán mã hóa được dùng như DES, 3DES, AES, RC2,…. | **Đối với mã khối**, khi mã hóa, dữ liệu ban đầu được chia thành các khối (block) thường có kích thước bằng nhau, và kích thước này sẽ tùy thuộc vào thuật toán mã hóa được dùng như DES, 3DES, AES, RC2,…. |
| 15 | 21 | Thực thể đảm nhiệm chức năng sinh dòng khóa này được gọi là *bộ sinh dòng khóa* (keystream generator) | Nên gọi là bộ sinh hay phần tử sinh ? |
| 16 | 22 | Về căn bản một thuật toán mã dòng thuộc về một trong hai loại, đó là: ***mã dòng đồng bộ*** (synchronous cipher), và ***mã dòng tự đồng bộ*** (self-synchronous cipher) hay còn có tên gọi khác là *bất đồng bộ* (asynchronous). Tuy nhiên, những người từ dự án eSTREAM đã cho một định nghĩa tổng quát hơn về mã dòng | Về căn bản một thuật toán mã dòng thuộc một trong hai loại : ***mã dòng đồng bộ*** (synchronous cipher), và ***mã dòng tự đồng bộ*** (self-synchronous cipher) hay còn có tên gọi khác là *mã* *bất đồng bộ* (asynchronous cipher). Tuy nhiên, những người thuộc dự án eSTREAM đã đưa ra một định nghĩa tổng quát hơn về mã dòng |
| 17 | 23 | .*Trạng thái* là giá trị của một tập hợp các biến mang lại duy nhất một sự mô tả cho trạng thái của thiết bị | Hai chữ” trạng thái” liên tục dễ làm người nghe bị rối ?  *Trạng thái* (state) là giá trị của một tập hợp các biến mang lại duy nhất một sự mô tả cho trạng thái của thiết bị |
| 18 | 23 | Chúng có thể chỉ đơn giản là phép XOR chẵng hạn | Chúng có thể chỉ đơn giản là phép XOR chẳng hạn |
| 19 | 24 | -Còn khi dùng mã dòng đồng bộ theo công thức mã hóa: . Suy ra công thức giải mã . Trong trường hợp bị thay đổi thì dễ dàng nhìn thấy quá trình giải mã chỉ bị lan truyền lỗi như đối với mã dòng tự đồng bộ. Tuy nhiên, khi bị mất, lúc đó chuỗi các ký tự bản mã bị thụt lùi lại một ký tự. Nghĩa là đóng vai trò của , đóng vai trò của … | Cái này phải hỏi ông kỹ lại nè : Trong trường hợp thay đổi thì lỗi giải mã chỉ xảy ra tại một bit sao gọi là “lan truyền lỗi như đối với mã dòng tự đồng bộ” |
| 20 | 24 | Nói cách khác, kể từ  tất cả các ký tự bản mã đều bị lỗi. Dẫn đến quá trình giải mã tất cả các ký tự sau đó đều bị lỗi. | Nói cách khác, kể từ trở về sau tất cả các ký tự bản mã đều bị lỗi. Dẫn đến quá trình giải mã tất cả các ký tự sau đó đều bị lỗi. |
| 21 | 26 | Sở dĩ kiến trúc mà dòng này được gọi là ***mã dòng đồng bộ không cộng*** | Sở dĩ kiến trúc mã dòng này được gọi là ***mã dòng đồng bộ không cộng***  Câu này cũng có nhiều từ không cần thiết như “Sở dĩ” “là bởi do” |
| 22 | 27 | Một điểm thuận lợi của nó là có thể phát hiện sự thay đổi của bản rõ bởi vì bản rõ được mã hóa theo từng khối | “sự thay đổi của bản rõ” là gì và ý nghĩa ? |
| 23 | 27 | một *phương pháp mã khối động* (dynamic block ciphering approach) được mô tả như dưới. Với phương pháp này một bộ sinh dòng khóa và một thuật toán mã khối (dùng một khóa) biết trước được kết hợp theo cách mà một số ký tự dòng khóa sinh ra của bộ sinh dòng khóa được dùng để làm ***khóa động*** của thuật toán mã khối cho mỗi khối bản rõ | một *phương pháp mã khối động* (dynamic block ciphering approach) sẽ được mô tả như bên dưới. Với phương pháp này , một bộ sinh dòng khóa và một thuật toán mã khối biết trước được kết hợp với nhau. Các ký tự dòng khóa sinh ra bởi bộ sinh dòng khóa sẽ được dùng để làm ***khóa động*** của thuật toán mã khối cho mỗi khối bản rõ |
| 24 | 27 | Vì vậy sự mã hóa và giải mã được thể hiện như: | Vì vậy công thức mã hóa và giải mã được thể hiện như sau: |
| 25 |  | *Trong kiến trúc mã dòng này, không nhất thiết yêu cầu một độ phức tạp tuyến tính (linear complexity) (xem phần: 2.6. Các khía cạnh mật mã của Sequences) lớn đối với dãy sinh ra của SG nếu thuật toán mã khối được thiết kế tốt. Nếu hệ thống được thiết kế tốt, dường như những tấn công được biết đối với mã dòng* cộn *và mã khối không áp dụng được cho hệ thống này. Để tấn công nó, cần đến những phương thức mới* | *Trong kiến trúc mã dòng này,thường không nhất thiết phải có một độ phức tạp tuyến tính (linear complexity) (xem phần: 2.6. Các khía cạnh mật mã của Sequences) lớn đối với dãy sinh ra của SG . Nếu hệ thống theo kiến trúc mã dòng đồng bộ không cộng được thiết kế tốt thì phần lớn những kiểu tấn công đã biết đối với mã dòng cộng và mã khối không áp dụng được cho hệ thống này. Để tấn công nó, ta cần dùng đến những phương thức mới.* |
| 26 | 29 | ***LFSR*** (xem thêm ở các phần sau của luận văn) | Nên ghi rõ là xem ở mục mấy |
| 27 | 30 | ***Kiểu CFB*** ở một mã khối còn được dùng cho quá trình thực hiện mã dòng | ***Kiểu CFB*** trong mã khối còn được dùng cho quá trình thực hiện mã dòng |
| 28 | 31 | Cũng với mục đích để giữ được các ưu điểm của cả hai loại mã dòng cộng và mã khối, nhưng cũng để triệt tiêu các khuyết điểm của cả hai phương pháp, hệ thống ***mã phân phối hợp tác*** (cooperatively distributed (CD) cipher) được thiết kế để đáp ứng mục đích này | Hệ thống ***mã phân phối hợp tác*** (cooperatively distributed (CD) cipher) được thiết kế nhằm mục đích giữ được các ưu điểm của cả hai loại mã dòng cộng và mã khối, nhưng đồng thời cũng triệt tiêu các khuyết điểm của cả hai phương pháp trên. |
| 29 | 32 |  |  |
| 30 |  | Hệ thống ***mã phân phối hợp tác*** (cooperatively distributed (CD) cipher) được thiết kế nhằm mục đích giữ được … | Hệ thống ***mã phân phối hợp tác*** (cooperatively distributed cipher) hay còn gọi là ***mã CD*** được thiết kế nhằm mục đích giữ được … |
| 31 | 32 | Có thể có trường hợp các hàm mã hóa *E*0*, …, Es-*1 giống nhau, nhưng trong trường hợp này các khóa *k0, …, ks-1* sẽ phải khác nhau từng đôi một | Có thể có trường hợp các hàm mã hóa *E*0*, …, Es-*1 giống nhau, nhưng khi đó các khóa *k0, …, ks-1* sẽ phải khác nhau từng đôi một |
| 32 | 32 | ***nó quyết định chọn một thuật toán mã khối nào cho việc mã hóa/giải mã một khối dữ liệu tại một thời điểm*** | Cái này có một chút rắc rối , nếu theo phần 2.1.5 trang 18 sách Number Theory thì phải ghi là  ***nó quyết định thành phần mã khối nào sẽ được dùng cho việc mã hóa/giải mã một khối dữ liệu tại một thời điểm*** |
| 33 | 33 | Nếu hệ thống được thiết kế đúng đắn, có thể có một mã rất mạnh bằng cách chọn một số các mã khối rất yếu và một bộ sinh dãy yếu | Nếu hệ thống được thiết kế đúng đắn, ta có thể tạo một mã CD rất mạnh từ một số mã khối rất yếu và một bộ sinh dãy yếu |
| 34 | 34 | . Cho hệ thống mã CD với hai thành phần mã khối, ***các tham số được chọn*** như sau | Cho hệ thống mã CD với hai thành phần mã khối, ***các tham số*** cần đạt các giá trị như sau : |
| 35 | 35 | *Nếu SG được thiết kế tốt, trong khi một số mã khối yếu có thể dùng được trong trường hợp này* | *Nếu SG được thiết kế tốt, mã CD có thể tận dụng được các mã khối yếu.* |
| 36 |  | Một số dễ thi hành (implement), nhưng tính an toàn của chúng có thể khó điều khiển. Một số an toàn chống lại các loại tấn công nào đó, nhưng có thể thi hành tương đối chậm | Một số dễ thi hành (implement), nhưng tính an toàn của chúng khó điều khiển. Một số an toàn chống lại các loại tấn công nào đó, nhưng lại thi hành tương đối chậm |
| 37 | 39 | trình máy bán hàng tự động | trình máy chơi bạc |
| 38 | 43 | ***generator bit số học*** | ***bit generator số học***  bộ sinh bit… |
| 39 | 45 | Generator có thể sử dụng bộ trộn kênh theo cách kết hợp hai chuỗi lại với nhau | Generator có thể sử dụng bộ trộn kênh theo cách kết hợp hai thanh ghi lại với nhau |
| 40 | 50 | Việc cài đặt Generator lọc sẽ phức tạp hơn loại generator kết hợp vì ta phải cài đặt thêm hàm *f*. Loại generator này cũng được áp dụng trong các phương pháp mã hóa dựa trên generator ZUC | Loại generator này cũng được áp dụng trong các phương pháp mã hóa dựa trên generator ZUC |
| 41 | 54 | *đa thức không tầm thường* | ???  Bậc > 0 |
| 42 | 59 | Ta nói một dãy trên một trường, nghĩa là tất cả các phần tử của dãy đó thuộc trường đó | Ta nói một dãy trên một trường nghĩa là tất cả các phần tử của dãy đó thuộc trường đó |
| 43 | 74 | Ta xem xét một tấn công. Để đơn giản hóa vấn đề, ta giả sử rằng dòng khóa ở dạng nhị phân. Với giả sử rằng độ phức tạp tuyến tính của dòng khóa của đối phương rất kém bền vững | Ta xem xét một cách tấn công như sau : giả sử rằng dòng khóa ở dạng nhị phân và độ phức tạp tuyến tính của dòng khóa của đối phương rất kém bền vững… |
| 44 |  | , một số thì khó cài đặt nhưng tính *an toàn* của chúng có thể dễ bị kiểm soát | Câu này hình như không phù hợp với cách hành văn  “chơi lại” |
| 45 | 79 | Còn ***độ phức tạp cầu***, đối với các dòng khóa | Còn với ***độ phức tạp cầu***, nếu các dòng khóa |
| 46 | 79 | Giả sử công bố kiến trúc generator của một mô hình mã dòng dùng generator LFSR | Giả sử khi công bố kiến trúc generator của một mô hình mã dòng dùng generator LFSR |
| 47 | 82 | Rõ ràng tổng quát hơn | Tổng quát hơn |
| 48 | 83 | Như vậy lưu ý rằng truth table có ***tính thứ tự***. | Lưu ý rằng truth table có ***tính thứ tự***. |
| 49 |  | Vectơ | Vector |
| 50 |  | *all-zero all-one* | Đồng thời các phần cho **0** là cho **1** là có thể thay thế thành cho **b** là cho **c** là không ?  Sai hệ quả 3.4.5  Điều chỉnh **1** và **0** |
| 51 | 105 | The direction of transmission | Xác định hướng chuyển dữ liệu là upload hay download . |
| 52 | 105 | The bearer identity | Xác định sóng mang (bearer) . |
| 53 |  |  | Định nghĩa ord(a) ??? |
| 54 |  | Cho là trường với *pm* phần tử, và  là một phần tử của nó, sao cho *m* phần tử:    độc lập tuyến tính. | Câu này muốn khẳng định cái gì ? |
| 55 | 69 | *Cho các ký hiệu như trên, ta luôn có* | Dòng này có cần thiết không khi ông đã giải thích kí hiệu đó là gì rồi |
| 56 |  | Công thức tổng LFSR |  |
| 57 | 62 | **if** deg(v) < deg(v) **then** | **if** deg(v) < deg(*u*) **then** |
| 58 | 67 |  |  |
| 59 |  | Thực nghiệm sai SAC | Đã fix |
| 60 |  |  |  |
| 61 |  |  |  |
| 62 |  |  |  |
| 63 |  |  |  |
| 64 |  |  |  |
| 65 |  |  |  |
| 66 |  |  |  |
| 67 |  |  |  |
| 68 |  |  |  |
| 69 |  |  |  |
| 70 |  |  |  |
| 71 |  |  |  |
| 72 |  |  |  |
| 73 |  |  |  |
| 74 |  |  |  |
| 75 |  |  |  |
| 76 |  |  |  |
| 77 |  |  |  |
| 78 |  |  |  |
| 79 |  |  |  |
| 80 |  |  |  |
| 81 |  |  |  |

**Slide:**

* Giới thiệu:
  + Lý do cần đến mã dòng
  + Mục tiêu của luận văn
    - Làm rõ trọng tâm của luận văn là mã dòng ZUC.
* Lý thuyết cơ bản mã dòng
  + Khái niệm mã dòng.
  + Sự khác biệt giữa mã dòng và mã khối.
  + Giới thiệu các kiến trúc mã dòng.
  + Giới thiệu các loại bộ sinh.
* Thiết kế kiến trúc ZUC.
  + LFSR
  + BR
  + Hàm phi tuyến
    - Sbox
    - L1,L2
  + 128-EEA3.
* Chương trình thực hiện
  + Mô hình ứng dụng.
  + Kết quả đạt được của chương trình.
  + So sánh tốc độ với mã khối AES.
* Tính an toàn của ZUC: Hàm *F*.
  + Tính phi tuyến.
  + Tiêu chuẩn SAC.
  + Tính đồng nhất sai phân.
  + Tính cân bằng.
* Nhận xét
  + Tốc độ mã dòng vs mã khối.
  + Tính an toàn mã dòng.
* Kết luận và hướng phát triển.
* Cảm ơn.