دانشگاه پیام نور

# مبانی امنیت اطلاعات


**دکتر علی شکیبا**

«عضو هیئت علمی دانشگاه ولی‌عصر رفسنجان»

**منصوره عشوریون**  **محمد تاری**

**امروزه کتاب‌خوانی و علم‌آموزی، نه تنها یک وظیفه ملی، که یک واجب دینی است.**[1]

**مقام معظم رهبری**

در عصر حاضر یکی از شاخصه‌های ارزیابی رشد، توسعه و پیشرفت فرهنگی هر کشوری میزان تولید کتاب، مطالعه و کتاب‌خوانی مردم آن مرز و بوم است. ایران اسلامی نیز از دیرباز تاکنون با داشتن تمدنی چندهزارساله و مراکز متعدد علمی، فرهنگی، کتابخانه‌های معتبر، علما و دانشمندان بزرگ با آثار ارزشمند تاریخی، سرآمد دولت‌ها و ملت‌های دیگر بوده و در عرصه فرهنگ و تمدن جهانی به‌سان خورشیدی تابناک همچنان می‌درخشد و با فرزندان نیک‌نهاد خویش هنرنمایی می‌کند. چه کسی است که در دنیا با دانشمندان فرزانه و نام‌آور ایرانی همچون ابوعلی سینا، ابوریحان بیرونی، فارابی، خوارزمی و ... همچنین شاعران برجسته‌ای نظیر فردوسی، سعدی، مولوی، حافظ و ... آشنا نباشد و در مقابل عظمت آنها سر تعظیم فرود نیاورد. تمامی این افتخارات ارزشمند، برگرفته از میزان عشق و علاقه فراوان ملت ما به فراگیری علم و دانش از طریق خواندن و مطالعه منابع و کتاب‌های گوناگون است. به شکرانه الهی، تاریخ و گذشته ما، همیشه درخشان و پربار است. ولی اکنون در این زمینه در چه جایگاهی قرار داریم؟ آمار و ارقام ارائه‌شده از سوی مجامع و سازمان‌های فرهنگی در مورد سرانه مطالعه هر ایرانی، برایمان چندان امیدوارکننده نمی‌باشد.

کتاب، دروازه‌ای به سوی گستره دانش و معرفت است و کتاب خوب، یکی از بهترین ابزارهای کمال بشری است. همه دستاوردهای بشر در سراسر عمر جهان، تا آنجا که قابل کتابت بوده است، در میان دست‌نوشته‌هایی است که انسان‌ها پدید آورده و می‌آورند. در این مجموعه بی‌نظیر، تعالیم الهی، درس‌های پیامبران به بشر، و همچنین علوم مختلفی است که سعادت بشر بدون آگاهی از آن‌ها امکان‌پذیر نیست. کسی که با دنیای زیبا و زندگی‌بخش کتاب ارتباط ندارد بی‌شک از مهم‌ترین دستاورد انسانی و نیز از بیشترین معارف الهی و بشری محروم است. با این دیدگاه، به‌روشنی می‌توان ارزش و مفهوم رمزی عمیق در این حقیقت تاریخی را دریافت که اولین خطاب خداوند متعال به پیامبر گرامی اسلام(ص) این است که »بخوان!« و در اولین

---

۱. پیام مقام معظم رهبری به مناسبت آغاز هفته کتاب ۷۲/۱۰/۴

سوره‌ای که بر آن فرستاده عظیم‌الشأن خداوند، فرود آمده، نام «قلم» به تجلیل یاد شده‌است: «إِقْرَأْ وَ رَبُّکَ الْاَکْرَمُ. اَلَّذی عَلَّمَ بِالْقَلَم» در اهمیت عنصر کتاب برای تکامل جامعه انسانی، همین بس که تمامی ادیان آسمانی و رجال بزرگ تاریخ بشری، از طریق کتاب جاودانه مانده‌اند.

دانشگاه پیام‌نور با گستره جغرافیایی ایران‌شمول خود با هدف آموزش برای همه، همه‌جا و همه‌وقت، به‌عنوان دانشگاهی کتاب‌محور در نظام آموزش عالی کشورمان، افتخار دارد جایگاه اندیشه‌سازی و خردورزی بخش عظیمی از جوانان جویای علم این مرز و بوم باشد. تلاش فراوانی در ایام طولانی فعالیت این دانشگاه انجام پذیرفته تا با بهره‌گیری از تجربه‌های گرانقدر استادان و صاحب‌نظران برجسته کشورمان، کتاب‌ها و منابع آموزشی درسی شاخص و خودآموز تولید شود. در آینده هم، این مهم با هدف ارتقای سطح علمی، روزآمدی و توجه بیشتر به نیازهای مخاطبان دانشگاه پیام‌نور با جدیت ادامه خواهد داشت. به‌طور قطع استفاده از نظرات استادان، صاحب‌نظران و دانشجویان محترم، ما را در انجام این وظیفه مهم و خطیر یاری‌رسان خواهد بود. پیشاپیش از تمامی عزیزانی که با نقد، تصحیح و پیشنهادهای خود ما را در انجام این وظیفه خطیر یاری می‌رسانند، سپاسگزاری می‌نماییم. لازم است از تمامی اندیشمندانی که تاکنون دانشگاه پیام‌نور را منزلگه اندیشه‌سازی خود دانسته و ما را در تولید کتاب و محتوای آموزشی درسی یاری نموده‌اند، صمیمانه قدردانی گردد. موفقیت و بهروزی تمامی دانشجویان و دانش‌پژوهان عزیز آرزوی همیشگی ما است.

**دانشگاه پیام‌نور**

## فهرست مطالب

## پیشگفتار

هدف از تدوین کتاب حاضر، آشنایی دانشجویان با مبانی امنیت اطلاعات و مسائل کلیدی آن است. هر چند کتاب‌هایی بسیار در این موضوع توسط بزرگان علم امنیت اطلاعات به رشتهٔ تحریر درآمده است، اما در این کتاب هدف این بوده است که با نگارشی روان و درعین‌حال غنی، مطالب به‌گونه‌ای ارائه گردند که مخاطبین بتوانند مطالب را مطالعه نموده و درک نمایند. مطالب این کتاب در یازده فصل ارائه شده‌اند: در فصل اول، به تعریف امنیت و الزامات پیاده‌سازی آن در سامانه‌های نرم‌افزاری و سخت‌افزاری پرداخته می‌شود. فصل دوم به مسئلهٔ کنترل دسترسی خواهد پرداخت و این مسئله را در لایه‌های مختلف مورد بررسی قرار می‌دهد. فصل سوم به‌طور خاص به امنیت در لایهٔ نرم‌افزار می‌پردازد و به‌صورت خلاصه، سازوکارهای برنامه‌نویسی ایمن را ارائه می‌نماید. در فصل‌های چهارم و پنجم، دو سنگ‌بنای علم رمزنگاری، یعنی رمزهای با کلید متقارن و رمزهای با کلید نامتقارن، ارائه می‌شوند. در فصل ششم، الگوریتم‌های درهم‌سازی به‌عنوان یکی دیگر از پایه‌های علم رمزنگاری مورد بررسی قرار گرفته‌اند. فصل‌های هفتم، هشتم و نهم به کاربردهای الگوریتم‌های پایه در طراحی خدمت‌های امنیتی مانند امضای‌دیجیتال، مدیریت و توزیع کلید و احرازهویت پرداخته‌اند. در فصل دهم، تهدیدات، حملات و آسیب‌پذیری‌ها در دنیای واقعی مورد بررسی قرار گرفته‌اند و راهکارهایی برای جلوگیری یا مقابله با آن‌ها ارائه شده‌اند. در فصل یازدهم، علاوه‌بر ارائهٔ راهنمایی کوچک برای استفاده از ابزار CrypTool 2.0، به مسئلهٔ زنجیرهٔ بلوکی و کاربردهای آن در ایجاد رمزارزها مانند بیت‌کوین پرداخته‌شده‌است.

برای همگان واضح است که موضوعات بسیار جذاب، بدیع و کاربردی در امنیت اطلاعات وجود دارند که حتی نام‌بردن از آن‌ها در یک نوشتار چند صد صفحه‌ای غیرممکن است. نویسندگان اثر حاضر، تلاش داشته‌اند تا مطالبی را در نوشتار حاضر درج نمایند که مخاطب علاقه‌مند بتواند پس از مطالعه و درک آن‌ها، سفر خود را در دنیای

علوم امنیت داده آغاز نماید. علاوه‌بر متن حاضر، صفحه‌ای در شبکهٔ جهانی اینترنت به آدرس http://infosecbook.ir فراهم‌شده‌است تا زمینهٔ ارتباط بین مؤلفین و مخاطبین را ایجاد نماید. علاوه‌براین، در این صفحه، به مرور، محتوای کمک درسی نیز برای نوشتار حاضر قرار خواهد گرفت. هر یک از مؤلفین بنا به تخصص، علاقه و تجربهٔ خود، نگارش بخشی از این کتاب را به‌عهده داشته‌اند. نگارش فصل‌های اول، سوم تا ششم، هشتم، دهم و یازدهم توسط نویسندهٔ اول و فصل‌های دوم، هفتم و نهم به‌صورت مشترک توسط نویسندگان دوم و سوم انجام‌شده‌است.

گرچه نگارندگان اثر حاضر تلاش داشته‌اند تا اثری با حداقل ایرادات و کاستی‌ها فراهم آورند، اما خود معترف‌اند که هیچ اثری زمینی بدون عیب نیست. بنابراین، مؤلفان کتاب امیدوارند خوانندگان این اثر، ایرادات، نظرات و پیشنهادهای خود را به نویسندگان ارسال نمایند تا در فرصت‌های آتی برای رفع آن‌ها اقدام شود.

**دکتر علی شکیبا، دانشگاه ولی‌عصر (عج) رفسنجان**

**منصوره عشوریون، دانشگاه پیام‌نور**

**محمد تاری، دانشگاه پیام‌نور**

**تابستان ۱۳۹۸ بهار ۱۴۰۰**

# فصل اول

# مقدمه‌ای بر مبانی امنیت اطلاعات

### هدف کلی

آشنایی با تعاریف، تهدیدها، حملات و استانداردهای رایج در امنیت اطلاعات

### هدف‌های یادگیری

انتظار می‌رود پس از خواندن این فصل بتوانید:

۱. مفاهیم اساسی در امنیت را تشریح نمایید.

۲. معماری امنیتی X.800 را توصیف نمایید.

۳. انواع تهدیدات و حملات را شرح دهید.

٤. اصول اساسی یک طراحی ایمن را شرح دهید.

۵. سازوکارهای امنیتی را شرح دهید.

### مقدمه

امنیت، موضوع اصلی کتاب حاضر است و در این کتاب به موضوعات مختلفی از حوزهٔ امنیت داده[1]، امنیت رایانه[2] و امنیت شبکه[3] خواهیم پرداخت. مجموعه‌ای از روش‌ها که برای حفظ امنیت داده، فارغ از شکل آن، به کار می‌روند، روش‌های امنیت داده نام دارند.

1. Data security
2. Computer security
3. Network security

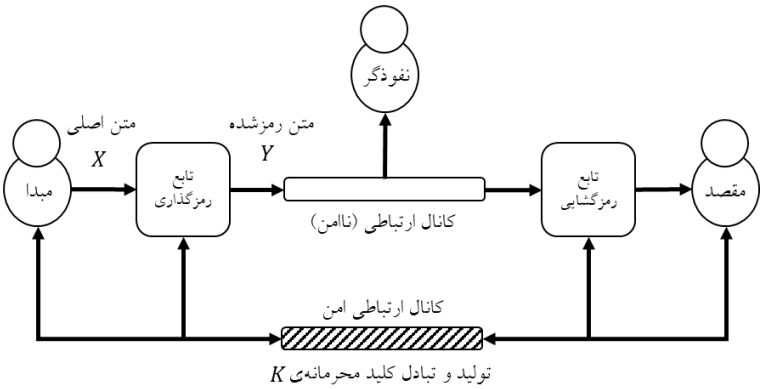
به‌عبارت‌دیگر، روش‌های برقراری امنیت داده، به داده دیجیتال و غیر دیجیتال قابل تعمیم هستند. در امنیت رایانه، به دنبال برقراری یک دستگاه رایانه، مانند رایانه‌های شخصی، خادم‌ها[1]، ابررایانه‌ها و حتی گوشی‌های تلفن همراه، هستیم. این دستگاه ممکن است به شبکه متصل باشد یا اتصالی به شبکه نداشته باشد. در امنیت شبکه، به تأمین امنیت مجموعه‌ای از دستگاه‌های رایانه‌ای که به هم متصل هستند به همراه ادوات شبکه‌ای می‌پردازیم. با این تفکیک اولیه، مباحث این کتاب در سه بخش قابل دسته‌بندی هستند: (۱) الگوریتم‌های رمزنگاری، (۲) قراردادهای ارتباطی و (۳) ابزارهای تأمین امنیت.

الگوریتم‌های رمزنگاری سنگ بنای امنیت هستند و در بخش امنیت داده مورد بررسی قرار می‌گیرند. این الگوریتم‌ها در سه زمینهٔ کلی قابل دسته‌بندی هستند: (۱) رمزنگاری‌های با کلید متقارن، (۲) رمزنگاری‌های با کلید نامتقارن، و (۳) الگوریتم‌های بررسی جامعیت داده. ساختار این الگوریتم‌ها به شدت وابسته به علوم ریاضی، مانند نظریهٔ اعداد، جبر و هندسه، و پیچیدگی محاسباتی هستند.

الگوریتم‌های رمزنگاری با کلید متقارن از پنج قسمت شامل (۱) کلید، (۲) الگوریتم رمزگذاری، (۳) الگوریتم رمزگشایی و (٤) متن اصلی و (٥) متن رمزشده تشکیل شده‌اند و برای یک متن اصلی، متن رمزشدهٔ معادل را تولید می‌کنند. شمای کلی این الگوریتم‌ها در شکل ۱-۱ آمده است. ازاین‌جهت که کلید مورداستفاده برای رمزگشایی و رمزگذاری یکسان است، به این نوع الگوریتم‌ها، الگوریتم‌های رمزنگاری با کلید متقارن گفته می‌شود. به‌عنوان نمونه‌ای از این الگوریتم‌ها، فرض کنید پیام X را در قطعه‌ای کاغذ نوشته‌شده‌است. به‌منظور رمزگذاری، آن پیام را در یک صندوق غیرقابل نفوذ قرار می‌دهیم و درب آن صندوق را قفل می‌کنیم. فرض کنید که تنها راه دسترسی به پیام قرار گرفته درون صندوق، استفاده از کلید و بازکردن درب صندوق باشد. حال صندوق را به مقصد ارسال می‌کنیم. در مقصد، دریافت‌کننده از کلید استفاده کرده و درب صندوق را باز می‌کند. سپس، وی می‌تواند به محتوای پیام دسترسی پیدا کند. در اینجا چند نکته

1. Server

قابل‌توجه است: (۱) لازم است تا کلید مورداستفاده برای صندوق، هم در مبدأ و هم در مقصد وجود داشته باشد. (۲) محرمانگی پیام وابسته به نفوذ ناپذیری صندوق و محرمانه‌بودن کلید است. به‌منظور تبادل کلید، لازم است تا طرفین ارتباط از یک کانال ارتباطی امن استفاده کنند. در فصل چهارم در مورد این الگوریتم‌ها بیشتر خواهید آموخت و در فصل هشتم، مسئلهٔ تبادل کلید به‌صورت دقیق بررسی خواهد شد.




**شکل ۱-۱.** طرح کلی یک الگوریتم رمزنگاری با کلید متقارن

علاوه‌بر الگوریتم‌های رمزنگاری با کلید متقارن، الگوریتم‌های رمزنگاری با کلید نامتقارن نیز وجود دارند. در این الگوریتم‌ها، از یک کلید برای رمزگذاری و از کلیدی دیگر برای رمزگشایی استفاده می‌شود. به دلیل تفاوت کلیدهای رمزگذاری و رمزگشایی، به این الگوریتم‌ها، الگوریتم‌های رمزنگاری با کلید نامتقارن[۱] نیز گفته می‌شود. برای نمونه، فرض کنید جعبه‌هایی نفوذناپذیر در اختیار داریم که درب آن‌ها توسط یک کلید قفل می‌شود و از کلید دیگری برای بازکردن قفل آن استفاده می‌شود. به‌عبارت‌دیگر، از کلید قفل‌کننده نمی‌توان برای بازکردن قفل جعبه استفاده کرد و از کلید بازکننده نیز نمی‌توان

۱. به الگوریتم‌های رمزنگاری با کلید نامتقارن، الگوریتم‌های کلید عمومی (Public-key) نیز گفته می‌شود. دقت داشته باشید که کلید رمزگذاری می‌تواند در کاربردهای امضای‌دیجیتال (فصل هفتم) به عنوان کلید خصوصی یا محرمانه در نظر گرفته شود و کلید رمزگشایی را به عنوان کلید عمومی در اختیار عموم قرار داد. درصورتی‌که در کاربرد حفظ محرمانگی، فصل پنجم، کلید رمزگذاری کلیدی عمومی است و کلید رمزگشایی یک کلید خصوصی محسوب می‌شود.

برای قفل‌کردن جعبه استفاده کرد. حال فرض کنید طرف A قصد دارد تا دیگران بتوانند برای وی پیامی را ارسال‌کنند. بنابراین جعبه‌های مربوط به خود را تولید می‌کند، کلید رمزگشایی را برای خود به‌صورت محرمانه نگهداری کرده و جعبه و کلید رمزگذاری را به‌صورت عمومی، در اختیار سایرین قرار می‌دهد. حال هر طرفی که بخواهد به طرف A پیامی را به‌صورت محرمانه ارسال کند، کافی است جعبهٔ طرف A را یافته و سپس پیام خود را در آن قرار دهد. سپس، با استفاده از کلید رمزگذاری، جعبه را قفل نماید و جعبه را ارسال کند. تنها کسی که می‌تواند قفل جعبه را باز کند، فردی است که کلید رمزگشا را در اختیار دارد. بنابراین، طرف A می‌تواند جعبه را بازگشایی نموده و محتوای پیام را دریافت کند. در مورد این الگوریتم‌ها در فصل پنجم بیشتر خواهید آموخت. البته این الگوریتم‌ها کاربردهایی اساسی در سایر مسائل مهم دنیای واقعی امنیت اطلاعات دارند که در فصل‌های هفتم تا نهم به‌تفصیل به آن‌ها پرداخته خواهد شد.

سومین دسته از الگوریتم‌های رمزنگاری، الگوریتم‌های جامعیت داده هستند. پایه‌ای‌ترین جزء در این الگوریتم‌ها، الگوریتم‌های درهم‌سازی[1] هستند. به‌صورت شهودی، این الگوریتم‌ها را می‌توان به دستگاه‌های آبمیوه‌گیری تشبیه کرد که چکیده‌ای از ورودی خود را تولید می‌کنند، به‌طوری که (۱) درصورتی‌که ورودی حتی به‌میزان یک بیت تغییر کند، خروجی بسیار متفاوت باشد، و (۲) با استفاده از چکیده نتوان ورودی را تشخیص داد. البته ویژگی‌های دیگری نیز برای این توابع مطرح است که در فصل ششم به‌صورت دقیق بررسی خواهند شد.

با ترکیب سه ساختار الگوریتم‌های رمزنگاری با کلید متقارن، الگوریتم‌های رمزنگاری با کلید نامتقارن، و الگوریتم‌های بررسی جامعیت داده می‌توان قراردادهای امنیت را ایجاد و از آن‌ها برای ایجاد ابزارهای تأمین امنیت داده استفاده نمود.

1. Hashing algorithms

## ۱-۱ مثلث C.I.A.

علاوه‌بر تعریف ارائه‌شده در ابتدای فصل از امنیت رایانه، تعریف دقیق‌تری نیز توسط مؤسسهٔ ملی استاندارد و فناوری آمریکا[1] ارائه‌شده‌است: «منظور از امنیت رایانه، ابزارها و کنترل‌هایی است که از محرمانگی[2]، جامعیت[3] و دردسترس‌بودن[4] سامانه‌های اطلاعاتی شامل سخت‌افزار، میان‌افزار، نرم‌افزار، اطلاعات مورد پردازش، ذخیره و تبادل‌شده اطمینان حاصل می‌کند». در این تعریف، از سه هدف کلیدی که به مثلث .C.I.A نیز معروف است، نام‌برده شده‌است. در محرمانگی، دو هدف مهم وجود دارد: (۱) اطلاعات خصوصی و مهم تنها در اختیار موجودیت‌های مجاز قرار گیرد و محتوای این اطلاعات برای سایر موجودیت‌ها فاش نشود. (۲) موجودیت‌ها مدیریت اطلاعات مربوط به خود را در اختیار داشته باشند و بدانند که این اطلاعات توسط چه کسانی و چگونه جمع‌آوری می‌شود و در اختیار چه کسانی و به چه منظوری قرار می‌گیرد. هدف اول، محرمانگی داده و هدف دوم را حریم‌خصوصی[5] گویند.

**مثال ۱:** *برای نمونه فرض کنید طرف $A$ قصد دارد تا پیام $X$ را به طرف $B$ ارسال نماید، به‌گونه‌ای که تنها $B$ بتواند از محتوای آن مطلع شود. در اینجا طرف سومی نیز به‌عنوان نفوذگر وجود دارد که هدف وی، کسب اطلاع از محتوای پیام $X$ است. به‌همین منظور، طرف $A$ پیام خود را به‌صورتی محرمانه به طرف $B$ منتقل می‌کند، به‌صورتی که تنها او به پیام دسترسی داشته باشد. البته بدیهی است ممکن است نفوذگر بتواند محتوای پیام را به تصادف حدس بزند. اما درصورتی‌که وی بتواند محتوای پیام رمزشده را بهتر از حدس‌زدن تشخیص دهد، محرمانگی خدشه‌دار شده‌است.*

**مثال ۲:** *فرض کنید طرف $A$ از یک پایگاه اطلاع‌رسانی بازدید می‌کند. در طی بازدید، وی به مجموعه‌ای از اخبار علاقه نشان داده و علاقهٔ خود را با کلیک بر روی*

1. National Institute of Security and Technology (NIST)
2. Confidentiality
3. Integrity
4. Availability
5. Privacy

*لینک‌ها و مطالعهٔ اخبار پی می‌گیرد. ممکن است زمان حضور وی در هر صفحه و قسمت‌هایی که بیشترین توجه وی به آن معطوف بوده است نیز ثبت شود. علاوه‌براین، آدرس IP او، ساعت ورود، مشخصات مرورگر و سامانهٔ عامل وی نیز ممکن است مورد ثبت قرار گیرد. اما این اطلاعات چه می‌شود؟ مهم‌تر از آن، این اطلاعات چگونه و تحت چه معیارهای امنیتی ذخیره می‌شوند و قرار است از آن‌ها چه استفاده‌ای شود؟ درصورتی‌که اطلاعات به‌درستی ذخیره و نگهداری نشوند، ممکن است بر اثر نفوذ، این اطلاعات فاش‌شده و هویت کاربران را به خطر اندازند. همچنین ممکن است کاربری تمایل نداشته باشد تا این اطلاعات در مورد وی جمع‌آوری شوند. درصورتی‌که یک سامانه اقدام به جمع‌آوری و ذخیره‌سازی اطلاعات بدون اطلاع و اجازهٔ کاربر نماید، آن سامانه دارای حریم خصوصی نیست. حتی اگر این اطلاعات با اطلاع و اجازهٔ کاربر ذخیره شوند، اما سازمان یا مالک آن پایگاه در نگهداری اطلاعات دقت کافی به عمل نیاورد و منجر به افشای اطلاعات کاربر شود، حریم خصوصی خدشه‌دار می‌شود. لازم به ذکر است که تعریف‌های متعددی از حریم‌خصوصی و سازوکارهای رعایت آن ارائه شده‌اند که از مقبول‌ترین آن‌ها می‌توان به حریم خصوصی تفاضلی[1] اشاره کرد.*

در جامعیت نیز از دو مفهوم استفاده می‌شود: (۱) جامعیت داده و (۲) جامعیت سامانه. در جامعیت داده، هدف تشخیص هرگونه تغییر در داده توسط موجودیت‌های غیرمجاز یا به شیوه‌های غیرمجاز است. در جامعیت سامانه، هدف اطمینان از عملکرد صحیح سامانه بدون مداخلهٔ موجودیت‌های غیرمجاز است.

**مثال ۳:** *فرض کنید طرف استاد درس مبانی امنیت اطلاعات، سرفصل درس را در ابتدای ترم منتشر می‌کند. نیاز نیست تا محرمانگی این اطلاعات حفظ شوند، اما ممکن است فردی قصد داشته باشد تا دانشجویان این استاد را با تغییر سرفصل منتشرشده گمراه*

---

۱. به صورت شهودی، حریم خصوصی تفاضلی (Differential Privacy) به این معنی است که درصورتی‌که دادهٔ یک کاربر در پایگاه داده باشد و پرس و جویی بر آن پایگاه داده اعمال شود، نتیجه تفاوت چندانی با حالتی که دادهٔ آن کاربر در پایگاه داده قرار ندارد، نداشته باشد. پرداختن به مدل‌های مختلف حریم‌خصوصی و روش‌های پیاده‌سازی آن‌ها موضوعی جذاب و داغ در صنعت و علم است که البته از حوصلهٔ متن حاضر خارج است.