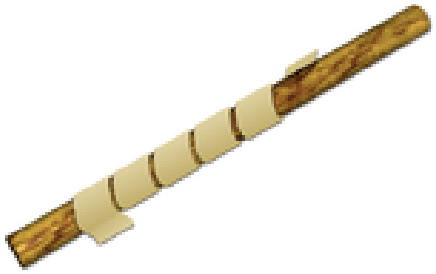
Cryptography

الگورتمهای رمزنگاری متقارن



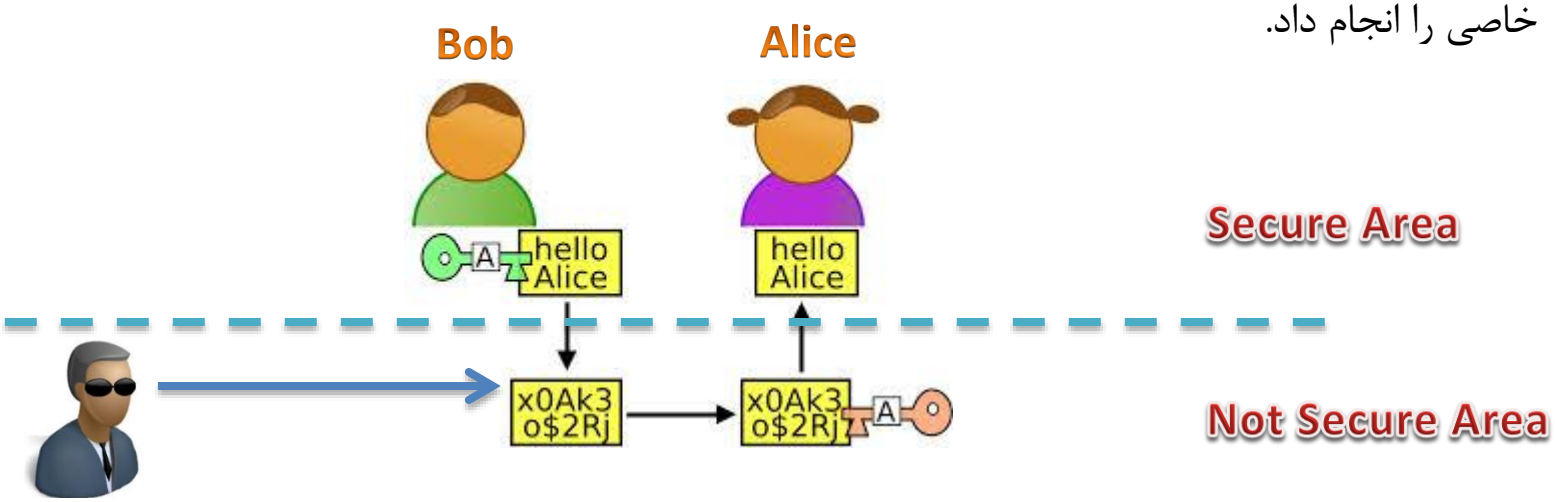
یکی دیگر از شیوه‌های رمزنگاری ابتدایی، پیچیدن یک نوار کاغذی بر روی استوانه‌ای با قطر مشخص و سپس نوشتن پیام روی کاغذ پیچیده شده بوده‌است. بدیهی است بدون اطلاع از مقدار قطر استوانه، خواندن پیام کار بسیار دشواری خواهد بود و تنها کسانی که نسخه‌های یکسانی از استوانه را داشته باشند می‌توانند پیام را بخوانند.

ماشین رمزکننده لورنتز که در جنگ جهانی دوم توسط آلمان برای رمز کردن پیام‌های نظامی مورد استفاده قرار گرفته‌است

مفهوم رمز نگاری

مفهوم سادهٔ رمز نگاری عبارت است از مبهم نمودن اطلاعات به طریقی که از دید فرد غیرمجاز پنهان شـود و در عین حال فرد مجاز قادر به مشاهده و استفاده از اطلاعات باشد.

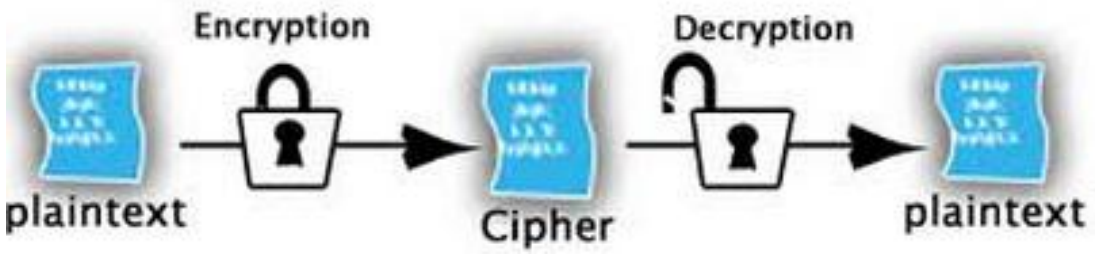
در رمزنگاری هدف ساختن طرح‌ها یا پروتکل‌هایی است که بتوان با کمک آنها حتی در حضور دشمن نیـز کارهـای خاصی را انجام داد.



یک هدف اساسی در رمزنگاری این است که به افراد این امکان را بدهند که روی یک کانال ناامن با حفظ حریم خصوصی و اصالت داده‌هایشان به صورت کاملاً امن با هم ارتباط برقرار کنند.

اصطلاحات رمزنگاری

- متن ساده - **Plain Text** - : اطلاعات به فرم اصلی اش را گویند.
- متن رمزی - **Cipher Text** - : اطلاعات مبهم شده توسط الگوریتم رمزنگاری.
- الگوریتم : روشی که متن ساده را به متن رمزی تبدیل می کند.
- کلید : دیتایی که الگوریتم بر طبق آن متن ساده را به متن رمزی تبدیل می کند و بالعکس.
- رمزنگاری - **Encryption** - : پروسه تبدیل متن ساده به متن رمزی.
- رمزگشایی - **Decryption** - : پروسهٔ تبدیل متن رمزی به متن ساده.



رمزنگاری

- رمزنگاری علاوه بر محرمانگی (Confidentiality) ، همچنین می‌تواند خواص امنیتی زیر را فراهم کند:
  - تصدیق (Authentication) : به طرفی که اطلاعات را می‌فرستد اعتبار و رسمیت می‌دهد.
  - جامعیت (Integrity) : اطمینان می‌دهد که اطلاعات در هنگام انتقال تغییر نیافته است.
  - عدم انکار (Non-Repudiation) : مانع از انکار یک طرف که پیامی فرستاده یا عملی را انجام داده است، می‌شود.

انواع الگوریتمهای رمزنگاری

انواع الگوریتمهای رمزنگاری

- الگوریتمهای منتشر نشده : Non-Published Algorithms

  برای مراکز نظامی ، مخابراتی ، تحقیقاتی و ...

- الگوریتمهای منتشر شده : Published Algorithms

  روش های تست شده و بررسی شده و تایید شده

انواع الگوریتمهای رمزنگاری

- Symmetric Algorithms الگورتمهای متقارن
- Asymmetric Algorithms الگورتمهای نامتقارن
- Hash Algorithms الگورتمهای درهم ریزی

انواع حملات رمزنگاری

- **Chiper Text Only**
  - مهاجم فقط متن رمز شده را در اختیار دارد .
- **Known Plain Text**
  - مهاجم متن رمز شده و متن اصلی متناظر را در اختیار دارد .
- **Chosen Plain text**
  - مهاجم این امکان را دارد که از تعداد محدودی متن متفاوت متن رمز شده متناظر را بدست آورد . در واقع در این روش مهاجم به طریقی به دستگاه یا برنامه رمز کننده دسترسی دارد .
- **Chosen Cipher text**
  - مهاجم این امکان را دارد که از تعداد ی متن رمز شده متفاوت متن اصلی متناظر را بدست آورد . در واقع در این روش مهاجم به طریقی به دستگاه یا برنامه رمز گشا دسترسی دارد .
- **Chosen text**
  - این روش ترکیب دو روش قبلی است . در واقع مهاجم به طریقی به دستگاه رمزگشا و رمزنگار دسترسی دارد .

رمزنگاری بلوکی

در این روش، اطلاعات با گروه‌های مختلف با طول معین تقسیم می‌شوند و هر گروه یا بلوک به صورت جداگانه رمزنگاری می‌شود. الگوریتم‌های معروفی که از این روش استفاده می‌کنند شامل DES، 3DESو AES هستند.

Data **E**ncryption **S**tandard

این الگوریتم از سوی سازمان ملی استانداردهای آمریکا (NBS)به عنوان الگوریتم رسمی برای استاندارد پردازش اطلاعات فدرال انتخاب شد و با این‌که این الگوریتم در بسیاری از کشورها استفاده می‌شود، الگوریتمی نا امن برای بسیاری از کاربردها به حساب می‌آید و این صرفا به علت طول کلید ۵۶ بیتی استفاده شده در آن است. در سال ۱۹۹۹ این الگوریتم در کمتر از ۲۳ ساعت با حمله brute force رمزگشایی شد. به همین دلیل الگوریتم ۳ DESطراحی شد که به نوعی همان الگوریتم DESاست که با ۳ کلید متفاوت هر بلوک را ۳ بار رمزنگاری می‌کند.

رمزنگاری بلوکی - DES

قدمهای اصلی DES این چنین هستند :

Initial Permutation (IP)

۱

- بلوک ۶۴ بیتی که می‌خواهد رمزشود، دستخوش یک **جایگشت** اولیه می‌شود؛ یعنی هر بیت به یک مکان جدید منتقل می‌شود.

به عنوان مثال، بیتهای یکم، دوم، و سوم به ترتیب به مکانهای، ۵۸ اُم ،۵۰ اُم ، و ۴۲ اُم منتقل می‌شوند.

۲

- ورودی ۶۴ بیتی دچار جایگشت شده به دو بلوک ۳۲ بیتی به نامهای چپ و راست، به ترتیب تقسیم می‌شود. مقادیر اولیهٔ بلوکهای چپ و راست با L0 و R0 مشخص می‌شوند.

۳

- سپس ۱۶ بار عملیات زیر روی بلوکهای L و R انجام می‌شود که در خلال هر تکرار (n از ۱ تا ۱۶ تغییر می‌کند)، فرمولهای زیر اعمال می‌شوند :

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \text{ XOR } f(R_{n-1}, K_n)$$

رمزنگاری بلوکی - DES

۳

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} \text{ XOR } f(R_{n-1}, K_n)$$

در هر گام داده‌شده از فرآیند، مقدار جدید بلوک L فقط از مقدار قبلی بلوک Rگرفته‌می‌شود. بلـوک جدیـد Rازمحاسـبهٔ XOR بلـوک قبلی L با نتایج اعمال تابع رمزکنندهٔ f بر بلوک قبلی R و Kn محاسبه می‌شود. (Kn یک مقدار ۴۸ بیتی مشتق‌شده از کلیـد ۶۴ بیتـی DES می‌باشد. هر مرحله، از ۴۸ بیت متفاوتی برحسب الگوریتم زمانبندی استاندارد کلید استفاده می‌کند.)

رمزنگاری بلوکی - DES

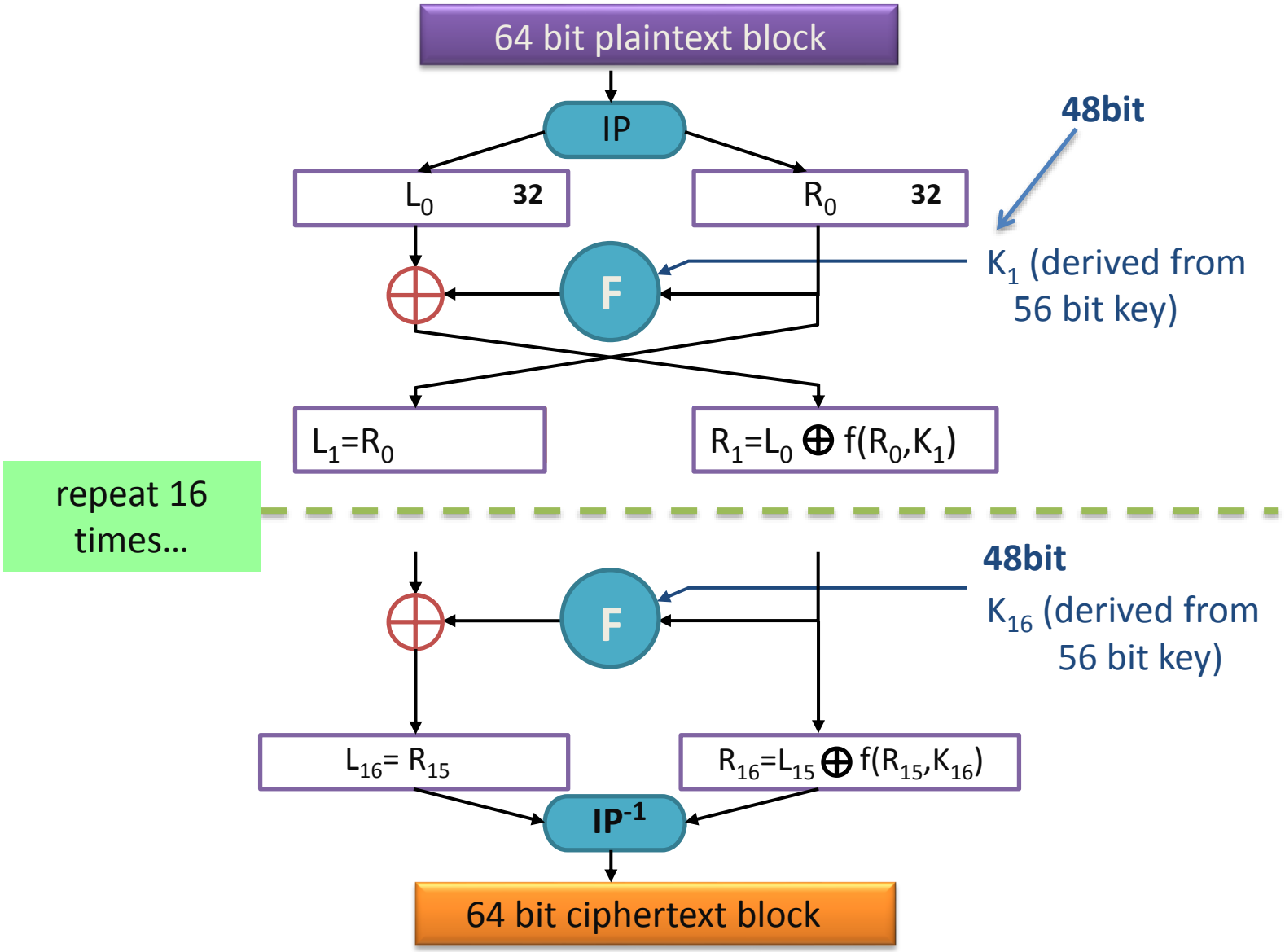
- تابع رمزکنندهٔ f ، مقدار ۳۲ بیتی بلوک R و زیرکلید ۴۸ بیتی را به روش زیر با هم ترکیب می‌کند . نخست ۳۲ بیت بلوک R بوسیلهٔ تابع بسط E به ۴۸ بیت بسط داده می‌شود؛ ۱۶ بیت اضافه با تکرار ۱۶ بیت از مکانهای از قبل تعریف شده مهیا می‌شوند.بلوک R بسط داده شده با زیرکلید ۴۸ بیتی OR می‌شود. حاصل، به ۸ بلوک ۶ بیتی تقسیم می‌شود. اینها به ورودی هشت S-box به نامهای S1 تا S8 اعمال می‌شوند. هر ورودی ۶ بیتی یک S-box با استفاده از یک جدول Lookup ، ۴ بیت خروجی را نتیجه می‌دهد. سپس خروجی ۳۲ بیتی مجموعهٔ S-box ها بوسیلهٔ تابع جایگشت P دوباره مرتب می‌شود.

۴

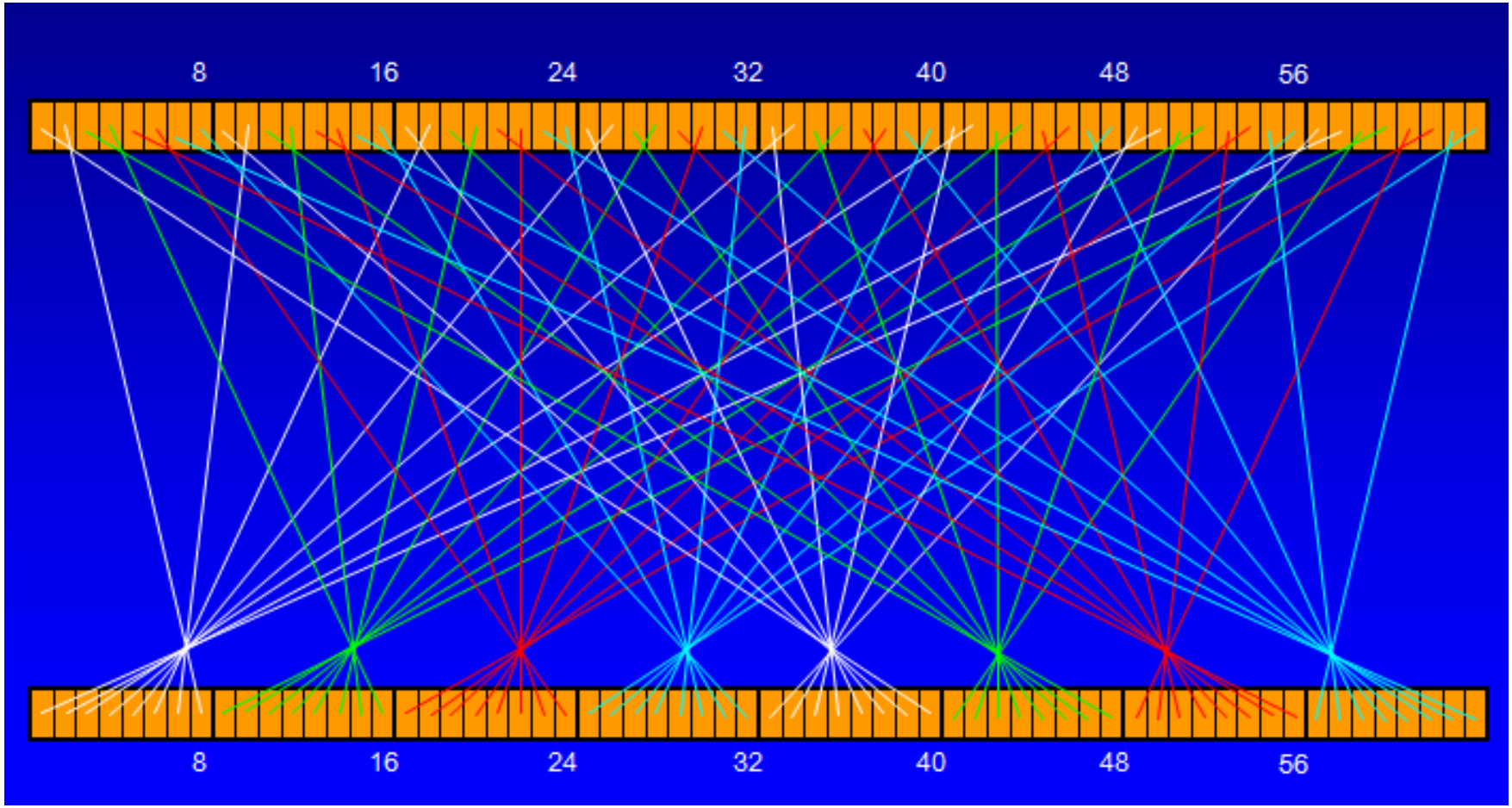
- نتایج، از دور نهایی DES - یعنی L16 و R16- به هدف یک مقدار ۶۴ بیتی با هم ترکیب می‌شوند وبه معکوس جایگشت اولیه (IP-1) وارد می‌شوند. در این گام، بیتها به مکانهای اصلی‌شان برگردانده می‌شوند. بنابراین بیتهای ۵۸ اُم، ۵۰ اُم، ۴۲ اُم ، به عنوان مثال، به مکانهای یکم، دوم، و سوم بازگردانده می‌شوند. خروجی IP-1 ، ۶۴ بیت متن رمز شده می‌باشد .

۵

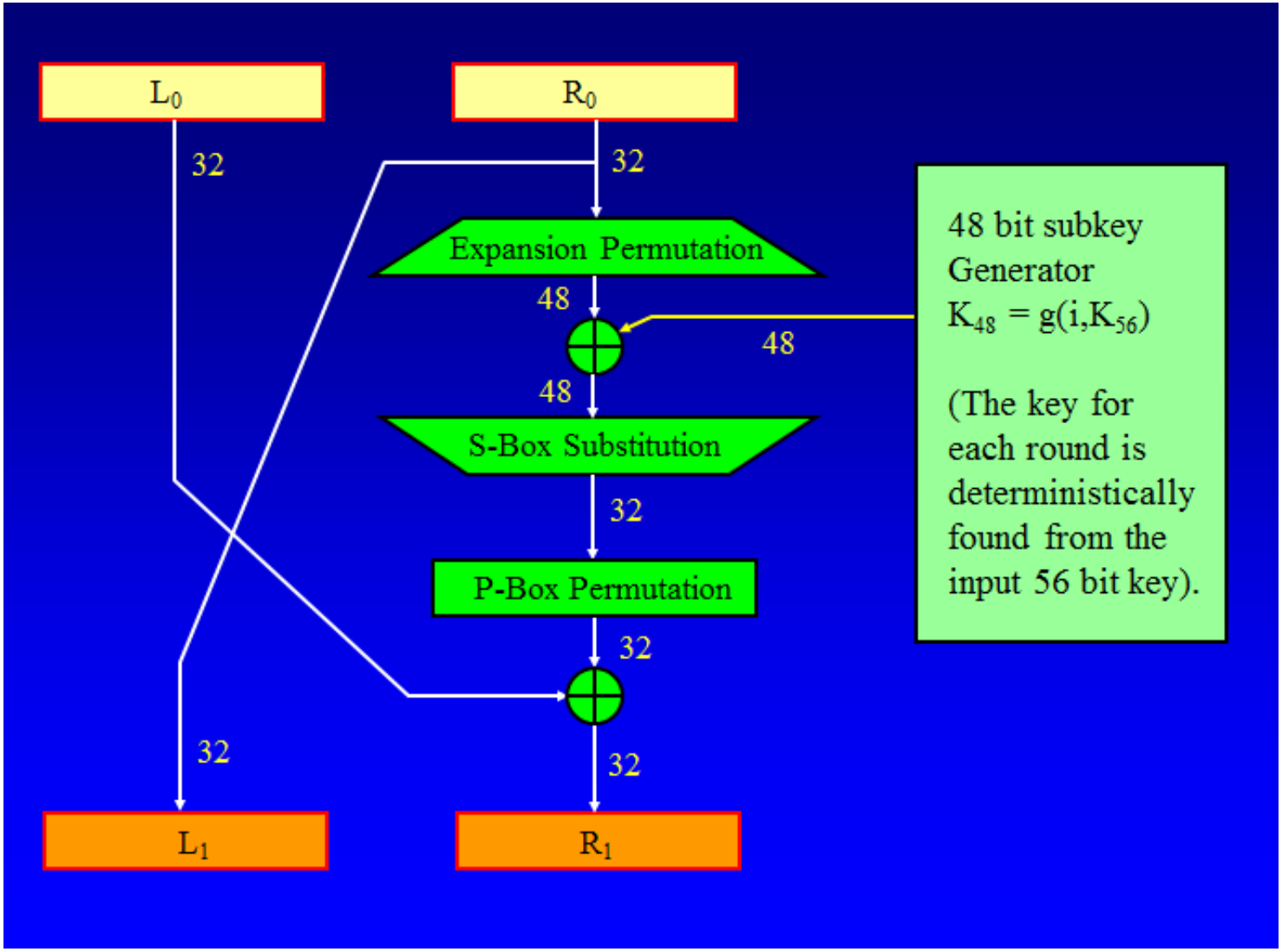
رمزنگاری بلوکی - DES



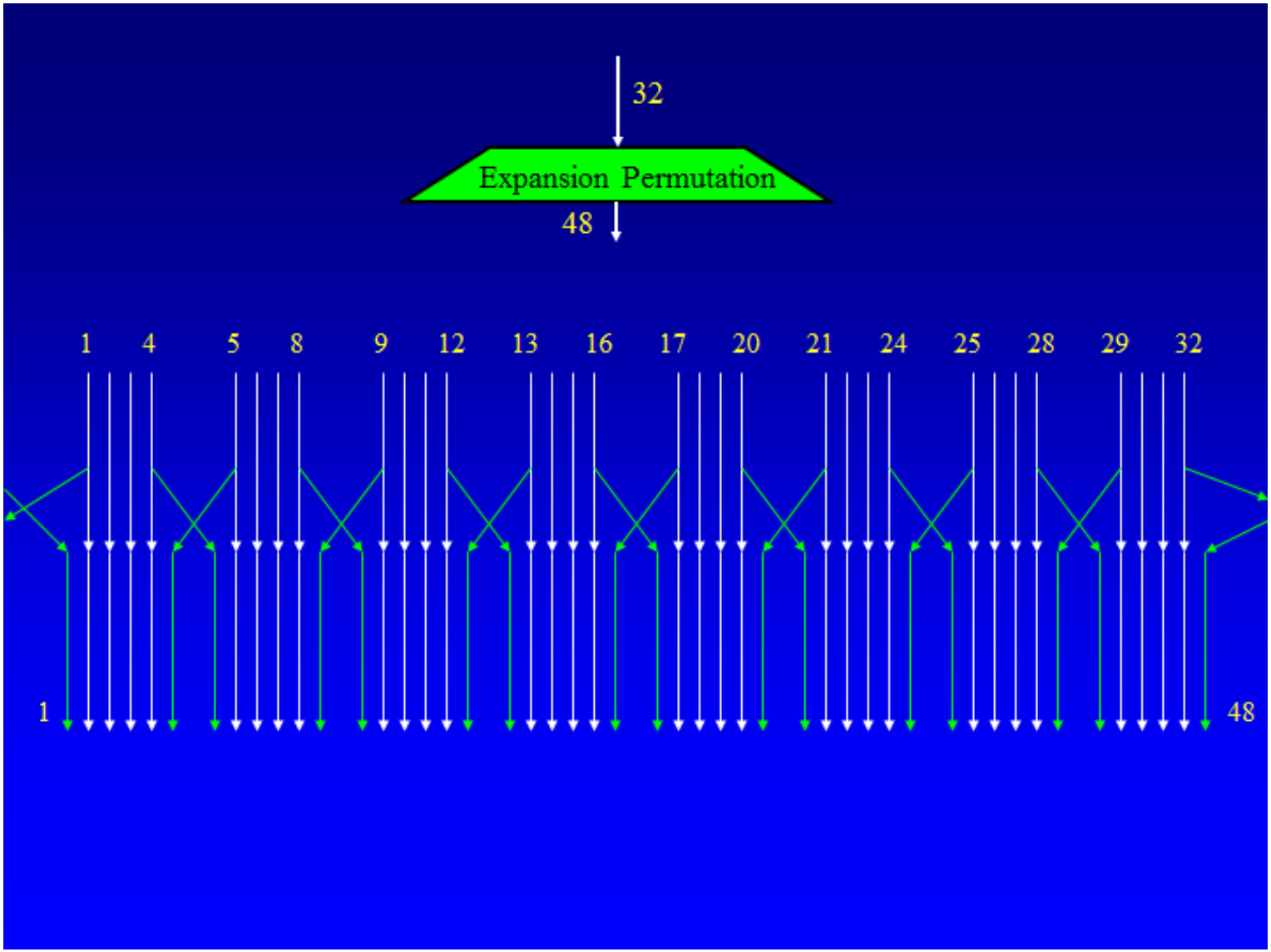
IP (Initial Permutation)



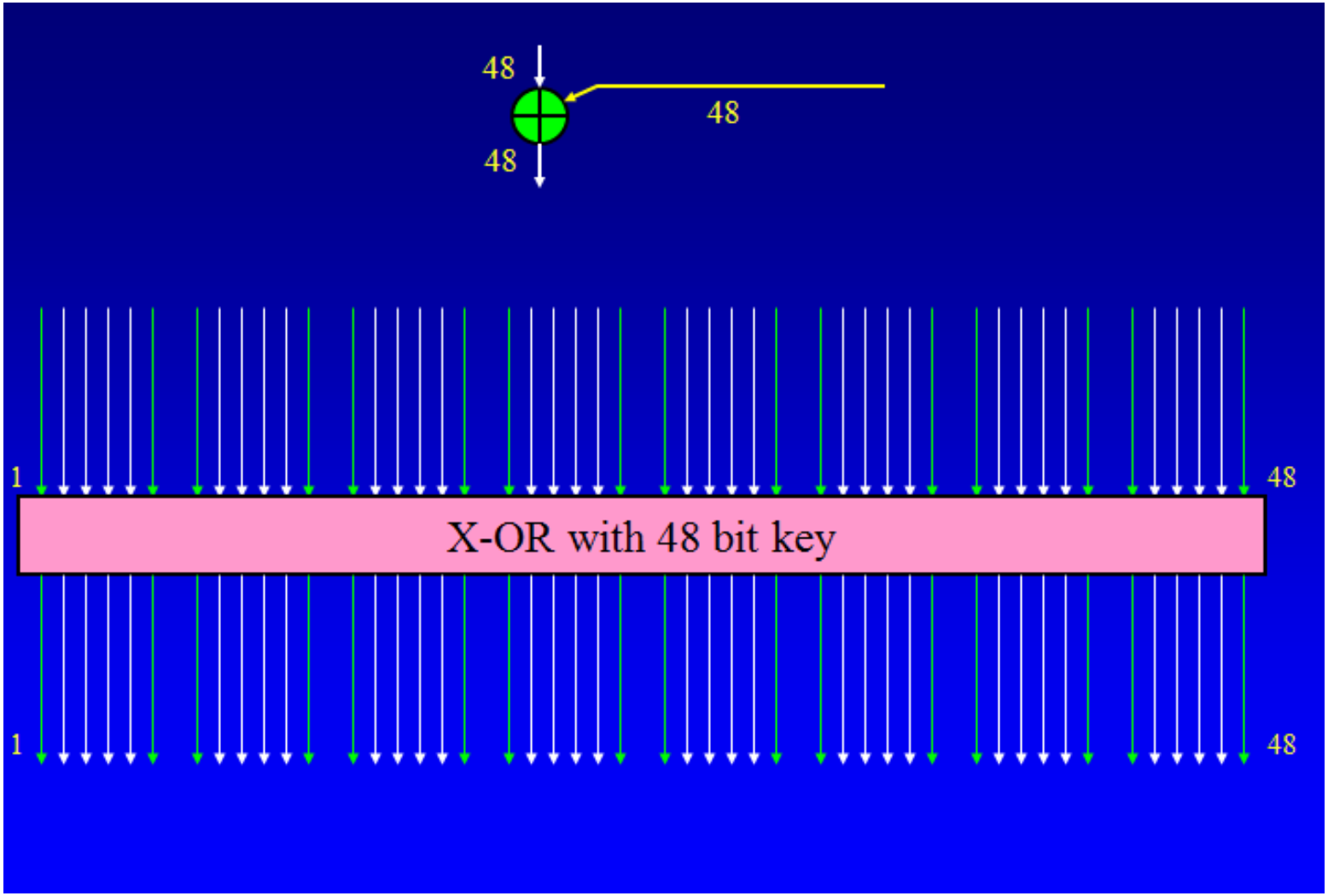
رمزنگاری بلوکی - DES



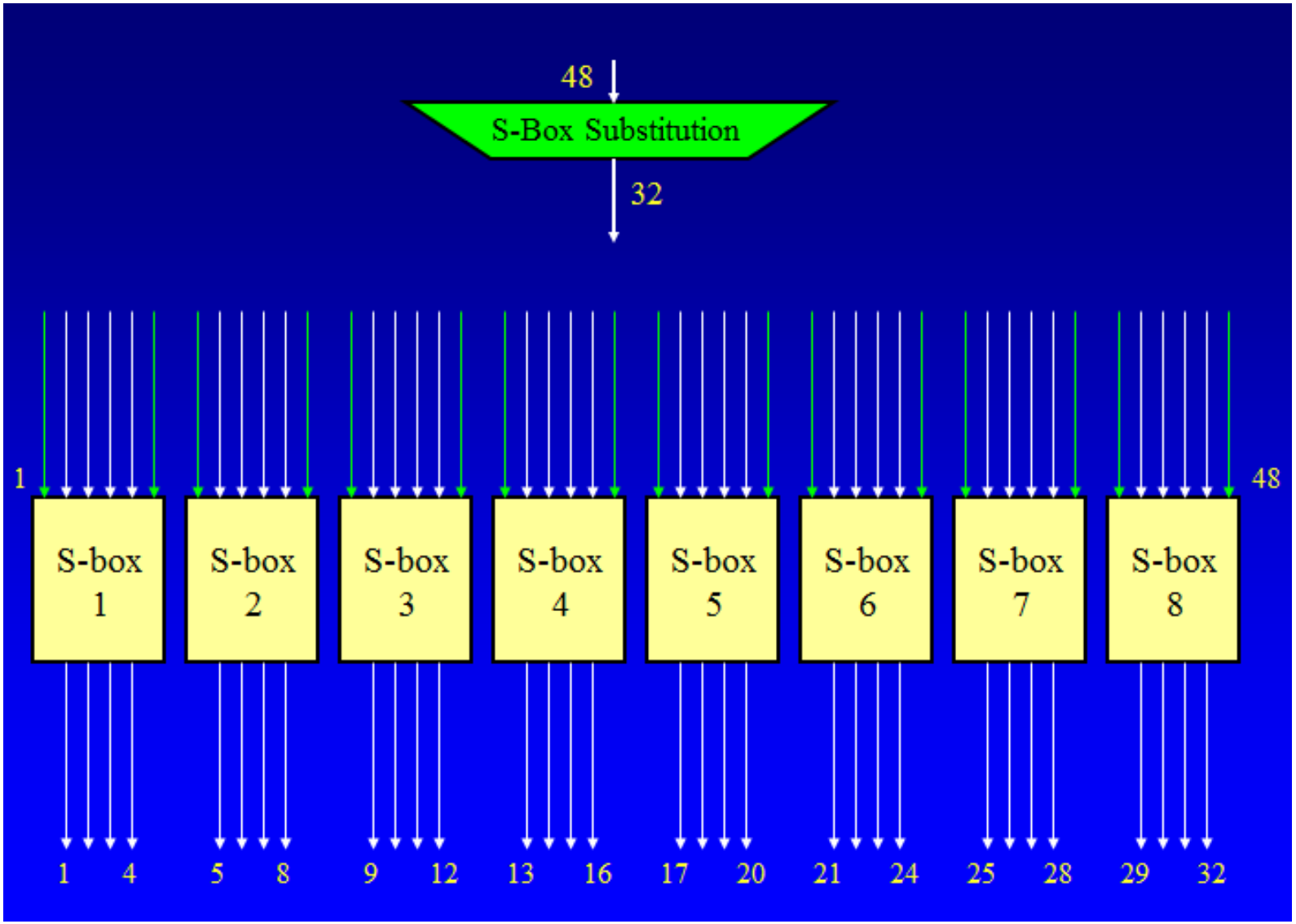
رمزنگاری بلوکی - DES



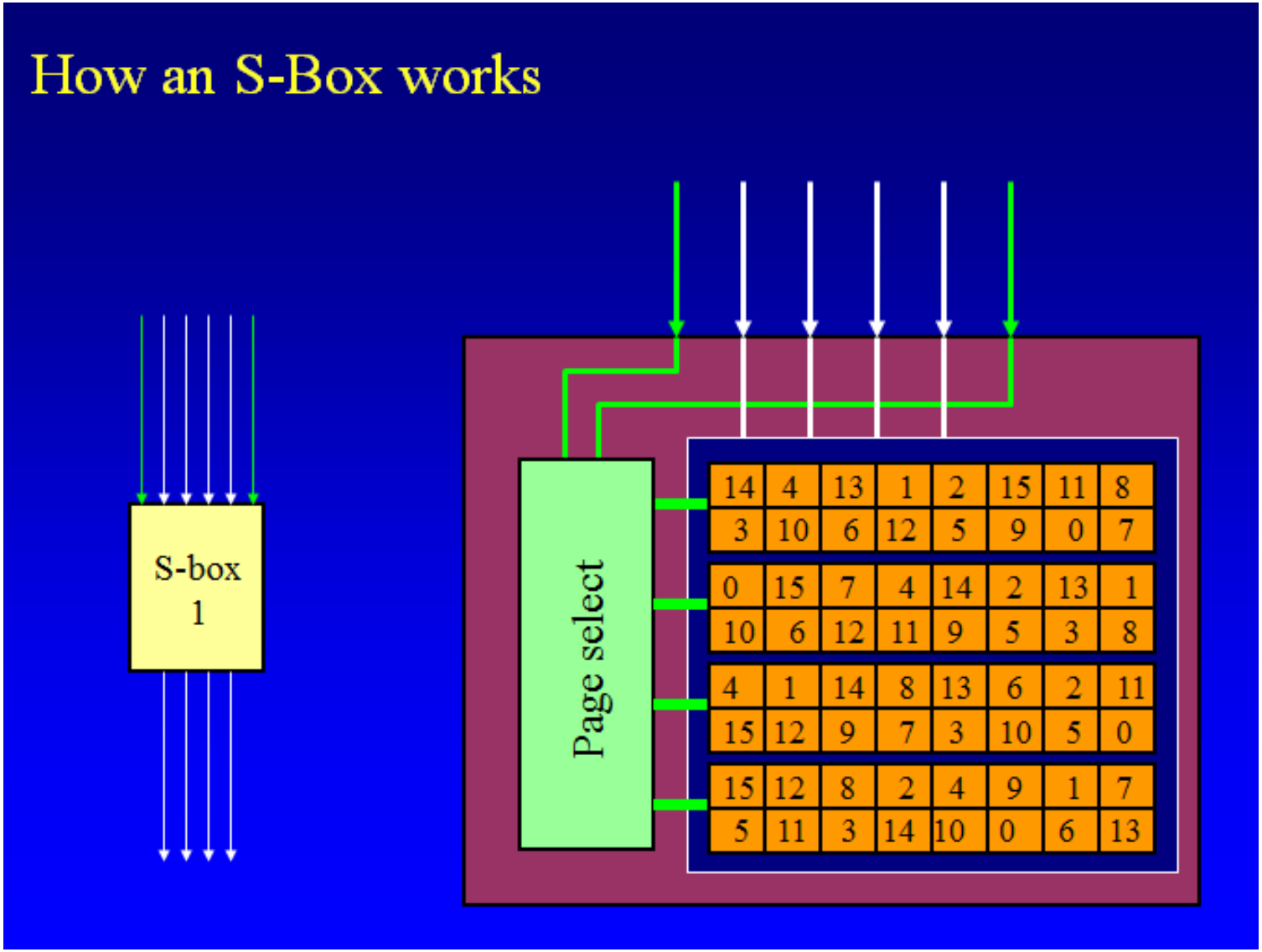
رمزنگاری بلوکی - DES



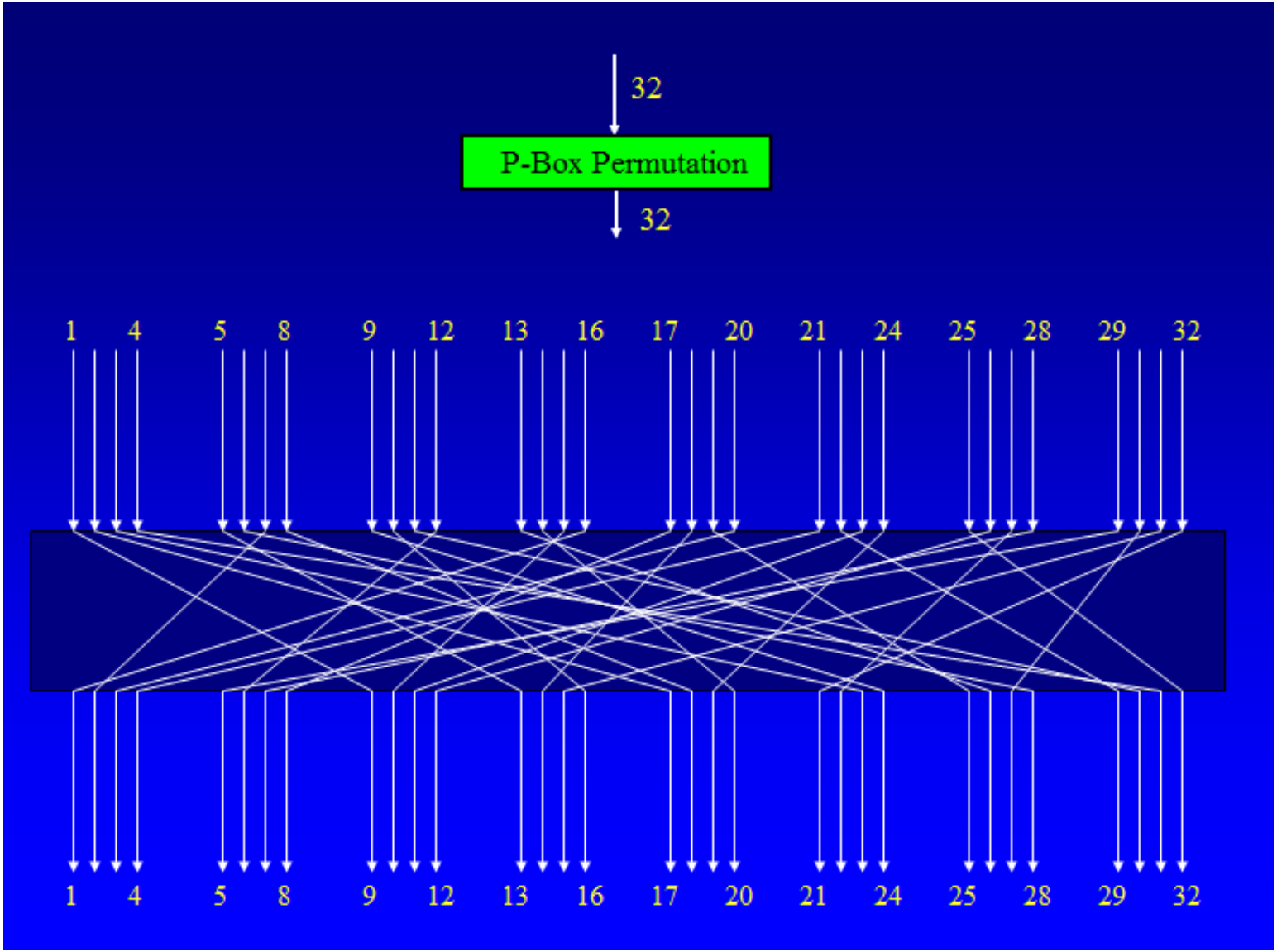
رمزنگاری بلوکی - DES



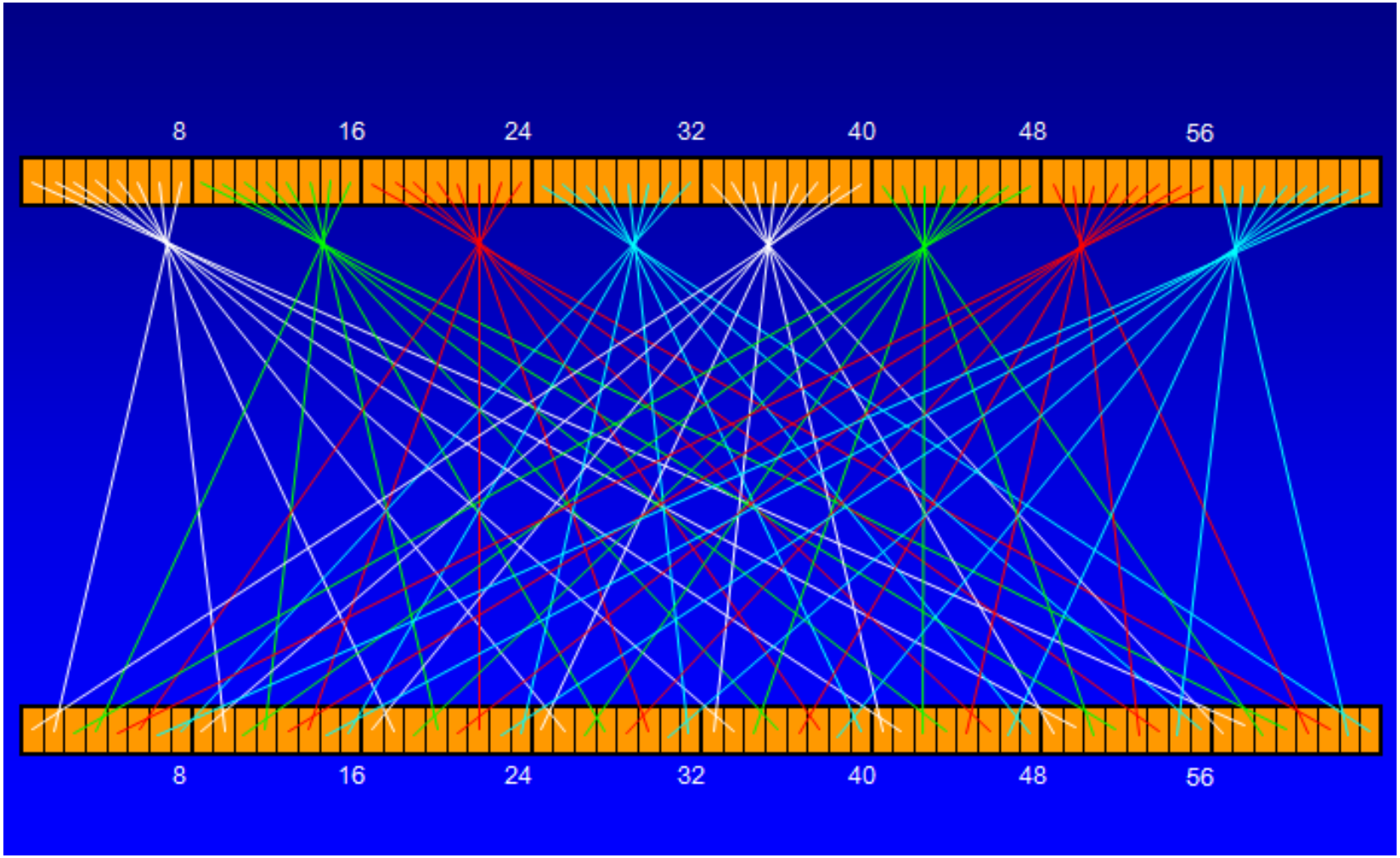
رمزنگاری بلوکی - DES



رمزنگاری بلوکی - DES



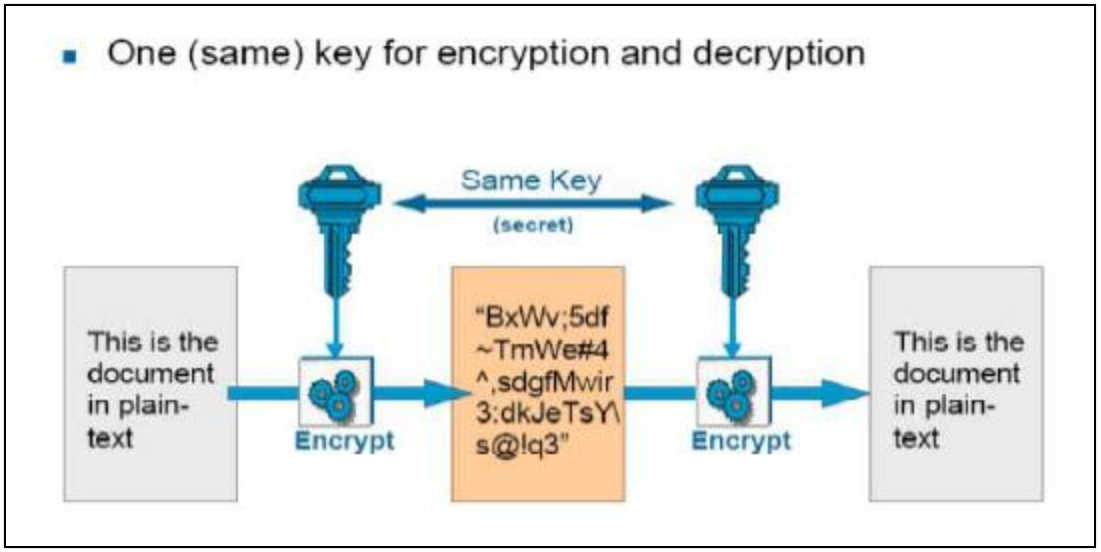
IP^{-1} (Final Permutation)



رمزنگاری بلوکی - DES

الگوریتمهای رمزنگاری متقارن

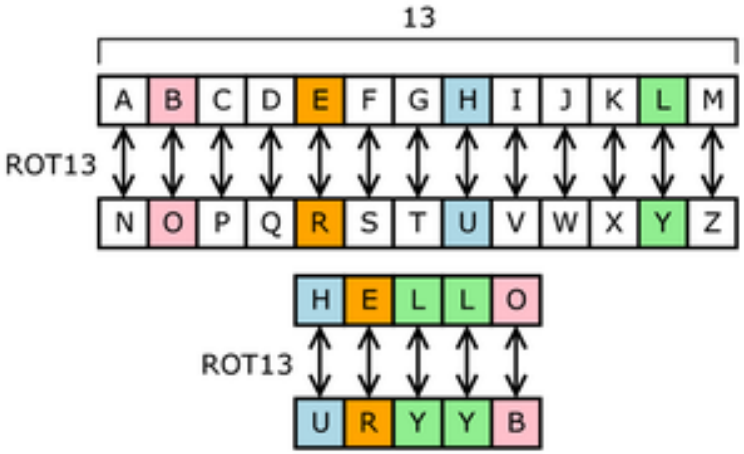
الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند.

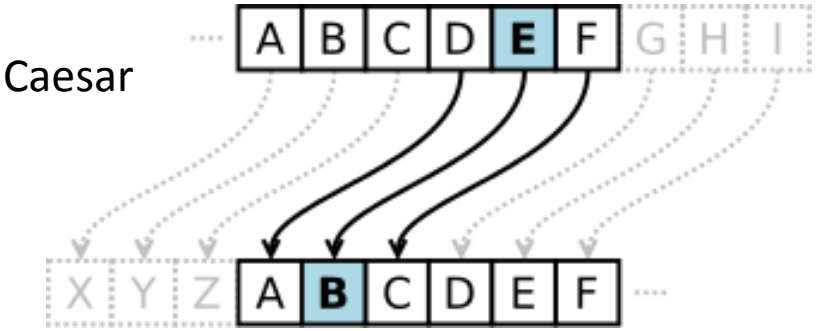


نقطه ظعف این الگوریتم آن است که توزیع کلید بین طرفین به صورت امن و مطمئن دشوار و پر هزینه است .

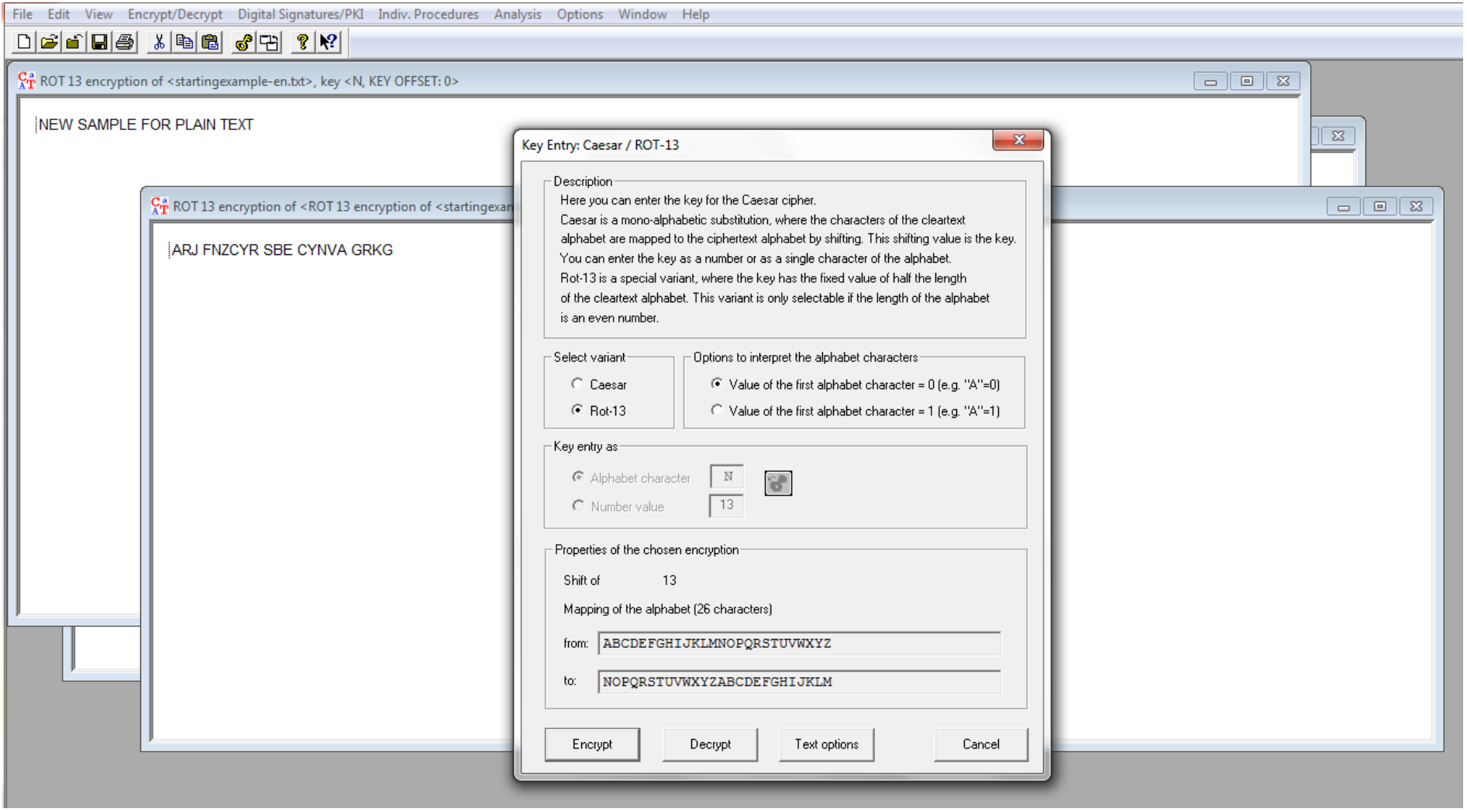
نقطه قوت این الگوریتم آن است که پردازش نسبتا کمتری برای رمزنگاری و رمز گشایی مورد نیاز است .

الگوریتم رمزنگاری CAESAR/ROT13





الگوریتم رمزنگاری CAESAR/ROT13



رمزنگاری ADFGVX

روش رمزنگاری ADFGVX در قدیم (سال 1918) توسط ارتش آلمان مورد استفاده قرار میگرفت .

الگوریتم رمزنگاری ADFGVX به شرح زیر میباشد . ابتدا یک جدول ۶*۶ شامل حروف و اعداد (۲۶ + ۱۰) به عنوان کلید رمزنگاری در نظر میگیریم . ترتیب قرار گرفتن حروف و اعداد می تواند بصورت تصادفی باشد . در اینصورت در مرحله اول رمزنگاری معادل هر حرف ترکیبی از دو حرف متناظر ستون و سطر جدول مذکور در نظر گرفته میشود .

	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	0	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	0	F	Q

For Example :

3 → **AF**

P → **AD**

Z → **FX**

رمزنگاری ADFGVX

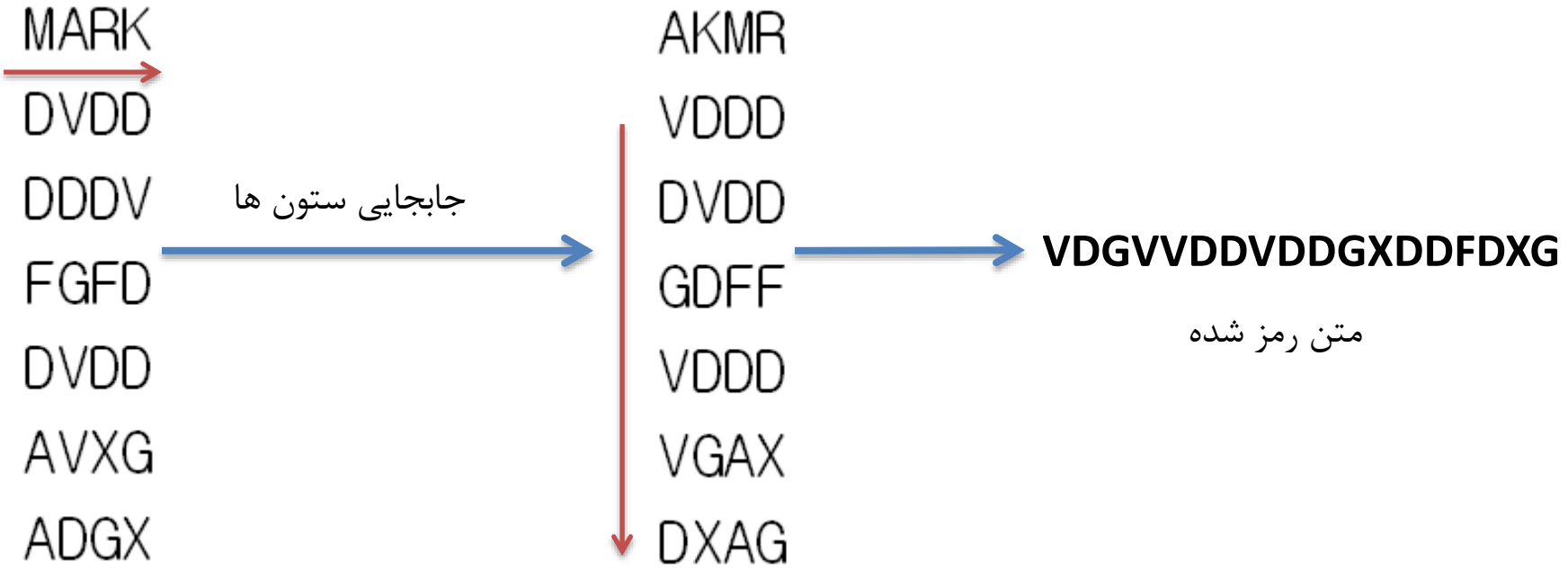
	A	D	F	G	V	X
A	8	P	3	D	1	N
D	L	T	4	0	A	H
F	7	K	B	C	5	Z
G	J	U	6	W	G	M
V	X	S	V	I	R	2
X	9	E	Y	O	F	Q

رمزنگاری ADFGVX

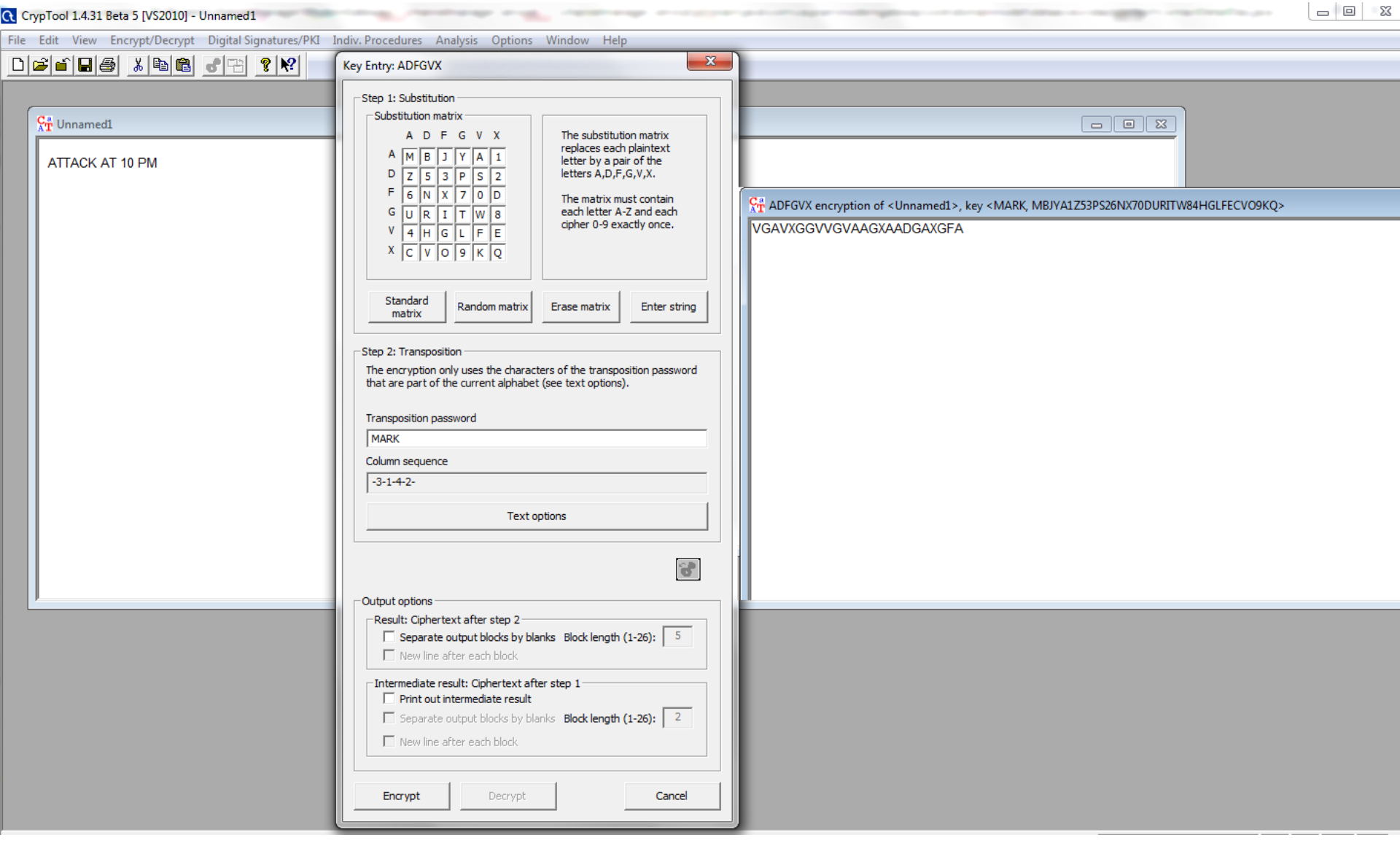
در مرحله بعد به تعداد دلخواه ستون در نظر میگیریم و متن رمز شده مرحله قبل را به ترتیب در آن قرار می دهیم .

و جای حروف را با تغییر و جابجایی ستون ها جابجا میکنیم . برای فهم بهتر در مثال زیر ۴ ستون و کلمه Mark

را در نظر میگیریم . پس از جابجایی ستونی حروف را به صورت ستونی پشت سر هم در نظر میگیریم .



رمزنگاری ADFGVX



رمزنگاری