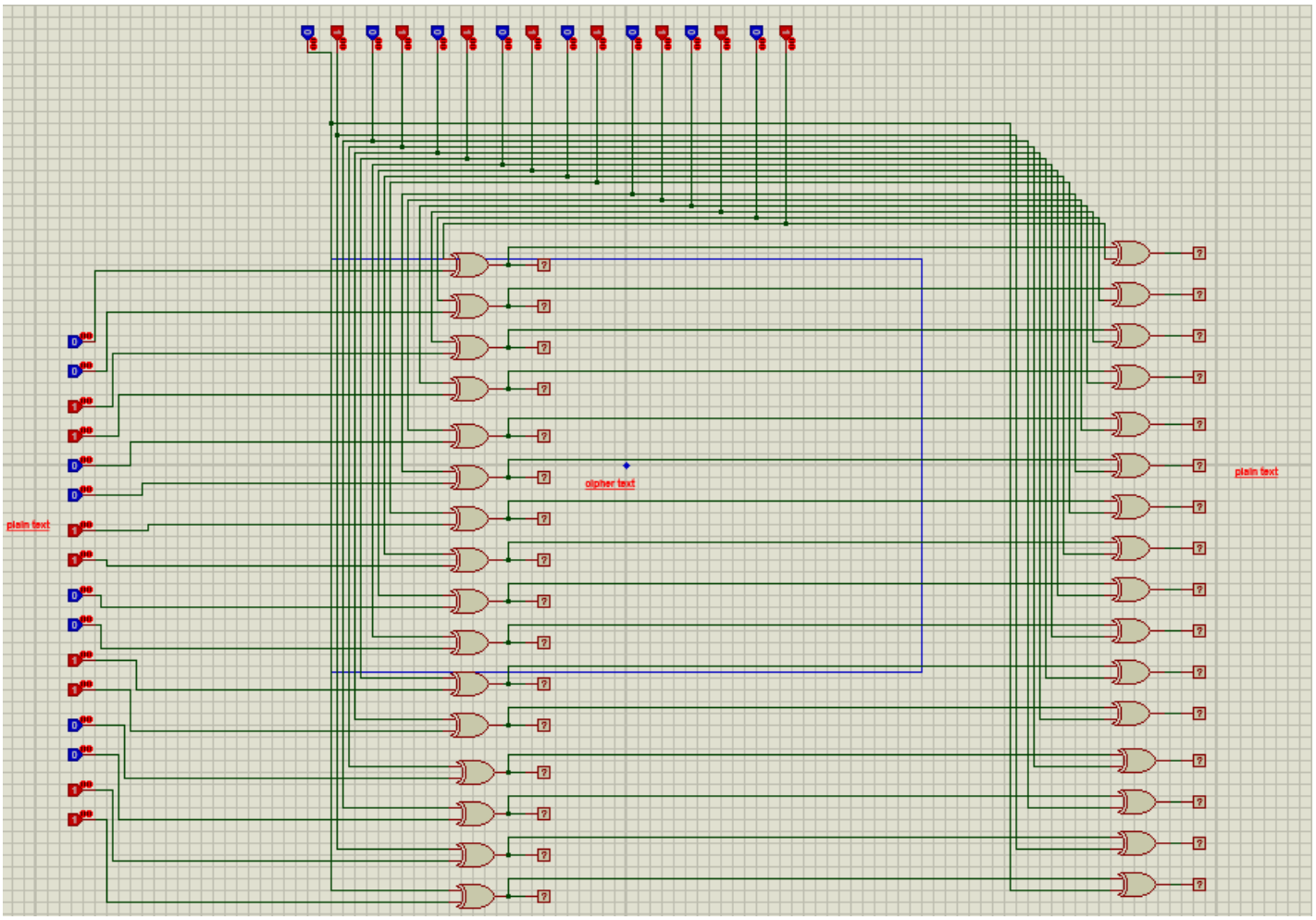

encryption-decryption circuit

سانیا مسعودی

فاطمه علیزاده

معصومه صنعت کار

رمزنگاری

رمزنگاری روشی است برای استفاده از اصول پیشرفته ریاضی در ذخیره و انتقال داده ها به شکلی خاص به طوری که فقط کسانی که در نظر گرفته شده باشند می توانند آن را بخوانند و پردازش کنند
نتیجه فرآیند رمزنگاری متن رمز (Ciphertext) نامیده می شود.
پیامی که باید رمزنگاری شود، متن آشکار (Plaintext)نامیده می شود و توسط یک تابع خاص به نام کلید (Key) به متن رمز، تبدیل می گردد .

رمزنگاری متقارن (symmetric)

یکی از الگوریتم‌های مورد استفاده رمزنگاری، رمزنگاری متقارن است که در آن ما از یک کلید یکسان برای رمزگذاری (Encryption) و همچنین رمزگشایی داده‌ها (Decryption) استفاده می‌کنیم.

رمزنگاری متقارن قالبی یا قطعه‌ای(Cipher Block)

در این روش اطلاعات به بلاک‌های کوچکتر متنی تبدیل شده و با استفاده از یک کلید مخفی خاص رمزگذاری می‌شوند.

- سه نوع از مهم ترین رمزهای قالبی متقارن

الگوریتم استاندارد رمزنگاری دیتا DES

الگوریتم DES سه گانه

الگوریتم استاندارد رمزنگاری پیشرفته AES

الگوریتم‌های رمزنگاری متقارن جریانی(Stream Cipher)

در این روش به جای بلاک بندی اطلاعات هر کاراکتر به تنهایی رمزگذاری می‌شود .

رمزنگاری نامتقارن (asymmetric)

رمزنگاری نامتقارن به رمزنگاری کلید عمومی نیز معروف است

رمزنگاری نامتقارن مشابه رمزنگاری متقارن است ، اما کمی پیچیده تر است.تفاوت اصلی آن با رمزنگاری متقارن استفاده از جفت کلید است. رمزنگاری نامتقارن به منظور رمزگذاری و رمزگشایی داده ها ، به جای یک کلید مشترک ، از جفت کلید استفاده می کند. جفت کلید از ۲ قسمت ، یک کلید عمومی و یک کلید خصوصی تشکیل شده است.

- **کلید خصوصی**

کلید خصوصی یک کلید مخفی است که برای رمزگذاری و رمزگشایی پیام ها استفاده می شود. کلید خصوصی همراه با کلید عمومی استفاده می شود. باید در همه زمان ها خصوصی نگه داشته شود و هرگز نباید با کسی به اشتراک گذاشته شود

- **کلید عمومی**

از کلید عمومی فقط برای رمزگذاری پیام استفاده می شود. می تواند برای افراد دیگر ارسال شود. هنگامی که فرستنده پیامی را با استفاده از کلید عمومی شما رمزگذاری کرد ، می توانید قفل آن را فقط با استفاده از کلید خصوصی خود باز کنید.

الگوریتم RSA

RSAتاکنون پرکاربردترین الگوریتم رمزگذاری نامتقارن بوده است. اساساً ، این روش شامل دو عدد اول تصادفی بزرگ است . این اعداد برای ایجاد عدد بسیار بزرگ دیگری ضرب می شوند

الگوریتم ECC

این روش که یکی دیگر از روش هاب رمزنگاری نامتقارن است از منحنی های بیضوی برای رمزنگاری استفاده میکند.

رمزنگاری با استفاده از گیت XOR

گیت XOR به دلیل خاصیت بازگشتی ای که دارد در رمزنگاری ها پرکاربرد است و رمزنگاری با استفاده از این گیت به صورت متقارن انجام میشود.

در این روش رمزنگاری، داده اولیه با یک کلید XOR میشود و سپس اگر داده رمزگشایی شده را با همان کلید XOR کنیم نتیجه خروجی، داده اول قبل از رمز گشایی خواهد بود.

Input		Output
A	B	F = AB′ + A′B
0	0	0
0	1	1
1	0	1
1	1	0

برای مثال عدد دوبیتی ۰۱ را اگر با کلید ۱۰ رمزنگاری کنیم نتیجه ۱۱ است و اگر ۱۱ را با ۱۰ XOR کنیم خروجی ۰۱ میباشد که همان عدد اول قبل از رمزنگاری است.