RSA:

RSA از اولین شیوه های رمزنگاری به روش کلید عمومی است که به صورت گسترده برای تامین امنیت انتقال داده استفاده می شود. در این چنین سیستم های رمزنگاری، کلید رمزگذاری عمومی است و از کلید رمزگشایی که مخفی است، جداست. در آراس‌اِی، این عدم تقارن مبتنی بر این است که تجزیه از عددی که ضرب دو عدد اول بزرگ است در عمل بسیار دشوار است.

این روش، نخستین روش مورد اعتماد در بین روش‌های رمزنگاری دیگر است و یکی از بزرگ‌ترین پیشرفت‌ها در زمینهٔ رمزنگاری به حساب می‌آید. آراس‌ای همچنان به صورت گسترده‌ای در تبادلات الکترونیکی استفاده می‌شود و در صورت استفاده درست با کلیدهای طولانی کاملاً امن به نظر می‌رسد.

حروف اولیهRSA ، حروف اولیه نام های خانوادگی Ron RIvest ، Adi Shamirو Adleman است که در سال ۱۹۷۷ این الگوریتم را به طور عمومی معرفی کردند. یک ریاضی دان انگلیسی به نامClifford Cocks ، که برای ستاد ارتباطات دولت بریتانیا کار می کرد، سیستمی معادل این سیستم را در سال ۱۹۷۳ پیاده سازی کرده بود، که تا سال ۱۹۷۳ به صورت محرمانه باقی ماند.

یک کاربرRSA ، یک کلید عمومی را بر اساس دو عدد اول بزرگ را همراه با یک مقدار تصادفی ساخته و به صورت عمومی منتشر می کند. هر کسی می تواند از این کلید عمومی برای رمزگذاری یک پیام استفاده کند، اما تنها کسی که آن دو عدد اولی که کلید بر اساس آن ها ساخته شده را می داند، قادر به رمزگشایی پیام است. شکستن رمزگذاری RSA به مسئله ی RSA معروف است. تاکنون هیچ روشی برای شکست دادن این سیستم(در صورت استفاده ی کلید به اندازه ی کافی بزرگ) منتشر نشده است.

RSA به صورت نسبی، الگوریتم کندی است و به همین علت، کمتر برای رمزگذاری مستقیم اطلاعات کاربر استفاده می شود. بیشتر اوقات، RSA کلید رمزگشایی شده را برای الگوریتم کلید متقارن انتقال می دهد که در عوض قادر است توده ای از عملیات رمزگذاری-رمزگشایی را با سرعتی بسیار بالاتر انجام دهد.

چگونگی کارکرد الگوریتم در این لینک در دسترس است : https://fa.wikipedia.org/wiki/%D8%A2%D8%B1%D8%A7%D8%B3%E2%80%8C%D8%A7%DB%8C

پیاده سازی در:cryptool

ابتدا در قسمت templates>>Cryptography>>Modern>>RSA Decryption Cipher را باز میکنیم.

در قسمت Ciphertext متن رمز شده ی 3C 00 93 00 87 00 69 00 92 00 93 00 C1 00 4F 00 56 00 69 00 92 00 76 00 02 01 A0 را وارد می کنیم. در قسمت RSA Key Generator، Source را Enter keys manually و Public modulus N را ۲۹۹ و Public exponent e را ۲۳ و Private key d را نیز ۲۳ در نظر میگیرمیم. با زدن کلید start متن رمز گشایی شده Sepide Omidvar خواهد بود.