https://teses.usp.br/teses/disponiveis/55/55136/tde-06042017-164507/publico/DanieleHelenaBonfim_revisada.pdf pagina 62

https://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/Fernando_TN17M2.pdf

https://www.lume.ufrgs.br/bitstream/handle/10183/110014/000951896.pdf

https://medium.com/@tarcisioma/algoritmo-de-criptografia-assim%C3%A9trica-rsa-c6254a3c7042

https://www.lambda3.com.br/2012/12/entendendo-de-verdade-a-criptografia-rsa/

https://cryptoid.com.br/banco-de-noticias/29196criptografia-simetrica-e-assimetrica/

http://campeche.inf.furb.br/tccs/2006-I/2006-1henriquetomasipiresvf.pdf

http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf

http://wsmartins.net/ermacs/poster_39.pdf

https://kryptazia.wordpress.com/criptografia/blowfish/

https://www.wikiwand.com/pt/Twofish

http://www.quadibloc.com/crypto/co040301.htm

A criptografia RSA (Esse nome indica a primeira letra do sobrenome de cada criador) foi criada em 1977 por 3 cientistas que trabalhavam no MIT: Ron **R**ivest, Adi **S**hamir e Leonard **A**dleman. Ela foi a primeira "criptografia assimétrica" criada até então, trouxe inovação por utilizar 2 chaves (uma publica e outra privada) durante o processo de criptografar e descriptografar uma informação. De forma resumida, a chave pública criptografa e a chave privada descriptografa. Essa criptografia é considerada mais eficiente e segura do que a simétrica, que é conhecida por utilizar apenas 1 chave publica durante todo o processo.

RSA foi um grande avanço para a época e é considerada, até hoje, uma das melhores e mais seguras criptografias ja criadas de todos os tempos. Com 1 chave, era necessário enviar a mesma chave do emissor para o receptor, podendo ser facilmente interceptava por terceiros durante esse processo. Agora, todos os usuários ja possuem uma chave privada especifica que somente elas tem acesso, então apenas quem possuir essa chave irá conseguir descriptografar a mensagem/informação.

Na imagem abaixo é mostrado o processo detalhado dessa criptografia, mas, resumidamente, utiliza-se de 2 números primos gigantescos que irão passar por inúmeros processos, para descobrir os valores iniciais é preciso fatorar inúmeras vezes

até chegar no valor inicial (esses valores seriam a "quebra" da chave, a senha),no entando esse processo é bem complexo e pode levar até anos para ser decifrado manualmente.

No RSA as chaves são geradas da seguinte maneira:

1. Escolha de forma aleatória dois números primos grandes ***p*** e ***q***, da ordem de 10^{100} no mínimo
2. Calcule ***n=pq***
3. Calcule a função totiente* em ***n: $\phi(n) = (p - 1)(q - 1)$***
4. Escolha um inteiro ***e*** tal que ***$1 < e < \phi(n)$***, de forma que ***e*** e ***$\phi(n)$*** sejam co-primos (ou seja, o único divisor comum seja 1)
5. 5 - Calcule ***d*** de forma que ***$de \equiv 1 \pmod{\phi(n)}$***, ou seja, ***d*** seja o inverso multiplicativo de ***e*** em ***$\pmod{\phi(n)}$***.

Por fim, temos: A chave pública: o par ***(n, e,)***, e a chave privada: a tripla ***(p, q, d)***.

A criptografia IDEA (International Data Encryption Algorithm) foi criada em 1991 na suiça por James Massey e Xueija Lai. Ele é criptografia simétrica (ou chave clássica), ou seja, utiliza-se de apenas uma chave pública (128 bits) para criptografar e descriptografar informações, também é classificado com cifra de blocos (agrupamento de bits de tamanho fixo, 64 bits no caso) . Basicamente a IDEA é uma DES só que mais rapida, tanto que foi criada com esse objetivo. Hoje em dia ela é amplamente utlizada em diversas áreas, esde comunicação segura até internet banking.

IDEA possui 4 modos de operação: ECB,CBC,CFB e OFB, sendo ECB considerado o menos eficaz. IDEA envolve muitos processos matemáticos durante a seu processo de criptografar, ele utiliza repetidamente as opereções: adição,multiplicação e XOR. As imagens abaixo ilustram o processo detalhadamente.

a) XOR bit-a-bit;

b) adição de inteiros módulo 2^{16}, com entradas e saídas tratadas como inteiros de 16 bits sem sinal, isto é, variáveis com valores somente positivos (*unsigned*);

c) multiplicação de inteiros módulo $2^{16} + 1$, com entradas e saídas tratadas como inteiros de 16 bits sem sinal, exceto o bloco constituído por zeros que é tratado como representação 2^{16}.

Estrutura do IDEA:

a) o texto claro de 64 bits é dividido em quatro partes;

b) a partir da chave de 128 bits são geradas 52 sub-chaves de 16 bits cada;

c) o IDEA é composto por oito rodadas, sendo que em cada rodada são aplicadas 6 sub-chaves, e a mesma sub-chave não é repetida;

d) ao final, os dados passam por uma transformação.

A criptografia Blowfish foi criada por Bruce Schneier em 1994, classificado com cifra de blocos (64 bits). Assim como o IDEA e a DES, ele é uma criptografia simétrica, ou seja, utiliza-se apenas uma chave publica. Um diferencial desse algoritmo é que ele é **GRATUITO e NÃO PATENTEADO**, considerado um dos melhores algoritmos de criptografia gratuito disponivel. Sua chave pode variar entre 32 a 448 bits, uma de suas devastagens é a necessidade de memória relativamente grande se comparada com outros algoritmos do mercado.

Blowfish é utilizado em alguns sistemas operacionais, como o linux, também pode ser utilizado em: gerenciamento de senhas, e-commerce e banco de dados.

De forma leiga, O processo do Blowfish é bem semelhante ao IDEA, utiliza-se de 3 operações matemáticas (adição,multiplicação e XOR) e na transformação da chave em sub-chave, fazendo aumentar o total de bits durante a operação. Uma parte do processo está na imagem abaixo:

A entrada para essa parte do algoritmo são 64 bits, que serão divididos em dois grupos de 32 bits, que serão chamados de xL e xR. As operações abaixo deverão ser feitas 16 vezes.

- xL = xL XOR Pi
- xR = F(xL) XOR xR
- Troca de xL com xR

Após a décima sexta iteração, é necessário trocar xL e xR mais uma vez (*troca de xL e xR*). Em seguida, são feitas as seguintes operações:

- R = xR XOR P17;
- xL = xL XOR P18.

O texto cifrado será a união desses dois grupos (xLxR). A função F segue os seguintes passos:

A criptografia Twofish foi sucessora do Blowfish, criada em 1998 também por Bruce Schneier. Esse algoritmo foi um dos cinco finalistas no concurso Advanced Encryption Standard (AES), infelizmente não chegou a ganhar. Assim como o Blowfish, ele tambem é um algoritmo de cifra de blocos (128 bits, diferente do seu antecessor que tinha 64 bits), criptografia simétrica com chave pública que varia entre 3 valores: 128,198 ou 256 bits. Assim como seu antecessor, Twofish também é gratuito e não tem patente. Processo semelhante ao do Blowfish.

O twofish proporcionou uma maior segurança se comparado com o Blowfish, isso se da graças ao grande aumento de bits na cifra de blocos.

A criptografia SAFER foi criada em xxxx por James Massey (um dos criadores da IDEA), é classificado como criptografia simétrica (apenas 1 chave publica) e tambem é uma cifra de blocos, algoritmo 100% focado na segurança. Existem várias versões desse algoritmo que variam a quantidade de bits, a seguir as versões existentes.

- Safer: 64 bits
- Safer SK: 64 bits, mais segurança
- Safer-128: 128 bits
- Safer SK-128: 128 bits, mais segurança

Resumidamente, o processo do algoritmo consiste em dividr a chave em varias sub-chaves e, logo em seguida, realizar 8 passos de operações (soma e XOR). Abaixo estão imagens da ordem dos 8 passos e um exemplo de sub-chave.

XOR, add, add, XOR, XOR, add, add, XOR

```
  1  45 226 147 190  69  21 174
120   3 135 164 184  56 207  63
  8 103   9 148 235  38 168 107
189  24  52  27 187 191 114 247
```