CHAVES E HASHES	CHAVES E HASHES
Onde as Chaves Privadas **são geradas**?	As Chave Privadas geralmente são geradas de 2 maneiras: **- No Próprio Computador de um usuário (via software):** Essa chave é gerada por através de sorteio num algoritmo passado ao próprio sistema operacional a pessoa; **- Por através de Hardwares Criptográficos:** Dispositivos capazes de gerar e armazenar chaves criptográficas como itokens em Pen Drivers e Cartões de Crédito;
Onde as Chaves Públicas **são geradas**?	As Chaves Públicas sempre **são geradas a partir da Chave Privada**, isso acontece geralmente no próprio software do usuário e geralmente por debaixo dos panos. Por exemplo no whatsapp, quando adicionamos o número de uma pessoa, o próprio aplicativo do whatsapp faz a verificação se aquela pessoa existe e envia para nós a chave pública daquela pessoa para que consigamos enviar mensagens para ela. Mas caso essa pessoa deseje não receber nossas mensagens basta ela travar a sua chave pública, o famoso "bloquear número do whatsapp".
Onde os HASHES **são gerados**?	Os HASHES são **gerados no algoritmo da aplicação responsável por enviar a mensagem**, como um servidor de e-mail por exemplo, dentro dele haverão algoritmos que irão calcular o HASH de acordo com os caracteres utilizados na mensagem do usuário e irão juntar o HASH á mensagem trancada, que só será aberta se o número HASH enviado bater com o número HASH informado ao destinatário.
Qual a **relevância do tamanho** das nossas Chaves e HASHES?	No caso das nossas Chaves e HASHES podemos dizer que o **tamanho é documento, pois quanto maior o tamanho, mais segura é uma chave ou HASH.** Podemos ilustrar isso com um cadeado numerado, um cadeado que contém apenas 4 campos de possibilidades para números de 0 a 9 poderá gerar 10.000 possibilidades, pode parecer muito para um ser humano tentar, mas imagine um computador que é capaz de calcular essas 10.000 possibilidades em menos de um segundo. Isso significa que quase que instantaneamente sua senha pode ser descoberta, por isso nossas chaves e HASHES precisam ser grandes quando falamos de tamanho binário.
Qual o **tamanho de Chaves Criptográficas e dos HASH** utilizadas hoje?	Devido ao alto poder de processamento dos computadores hoje, a grande maioria dos sistemas de criptografia trabalha com **Chaves e HASHES de 256 bits**, essa chave é segura por que ela é capaz de gerar a seguinte quantidade de possibilidades: **115.792.089.237.316.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000** ou **1,15 x 10 (elevado a 77 vezes)** Para se ter ideia do poder criptográfico de uma chave como essa, se pegássemos um dos computadores mais potentes do mundo, que é capaz de testar 1.000.000.000.000.000 de chaves por segundo, para que ele conseguisse testar todas essas possibilidades acima ele levaria **8.810.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000 anos.** E pensar que hoje já possuimos chaves com 1024 bits!
Qual seria a **única maneira de uma pessoa descobrir** uma Chave ou um HASH?	A única maneira é partindo para um **ataque de força bruta**, por através de algoritmos que calculem vários testes consecutivos sobre as possibilidades de combinações da Chave ou do HASH. Lembrando que esse ataque só faz sentido se é feito sobre o HASH - para conseguir abrir a mensagem - ou sobre a Chave Privada - visto que descobrir a Chave Pública não adiantaria de nada, não conseguiriamos descobrir a Chave Privada a partir dela, e só descobriríamos a chave usada para criptografar uma mensagem - se não por esses dois métodos, seria inútil.
O que uma pessoa teria que **fazer para que um sistema de segurança destinatário acreditasse que uma mensagem falsa que ele recebeu é verdadeira**?	**- Encontrar a Chave Privada de uma Assinatura Digital:** sem chave privada, nada de assinatura autenticada, no momento em que a mensagem batesse no destinatário ela seria recusada; **- Encontrar a Chave Pública da Criptografia:** para conseguir enviar uma mensagem a pessoa desejada, utilizando a sua própria Chave Pública; **- Modificar o HASH antes da mensagem ser enviada:** Não dá para alterar o conteúdo de uma mensagem sem alterar o HASH, seria impossível;
O que é o **PIN**? E que relevância ele tem sobre as Chaves Privadas de Assinaturas Digitais?	**PIN:** Ou **Personal Identification Number (Número de Identificação Personalizada)** é uma senha utilizada para desbloqueio de Chave Privada em Assinaturas Digitais, ou seja, antes de assinar uma mensagem, a aplicação pede pelo PIN - **a autorização do uso da Chave Privada do usuário - sem o PIN, a chave não pode ser utilizada.** Nem sempre vamos usar o PIN, ele é mais utilizado em transações bancárias e aplicações com alto níveis de segurança.
O que é o **PUK**?	**PUK:** Ou **PIN Unlock Key (Chave de Desbloqueio do PIN)**, todo PIN tem um limite de tentativas ao colocar a senha, geralmente esse limite é 10 vezes, mas isso varia de sistema para sistema, por exemplo, sistemas bancários só aceitam 3 tentativas para os seus cartões. Quando o usuário usa todas as tentativas o seu cartão é travado, ou seja, sua **Chave Privada é perdida e nunca mais poderá ser utilizada, para gerar uma nova chave será necessário usar o PUK, que é uma senha para geração de uma nova Chave Privada para o seu PIN.** O PUK geralmente fica no poder do responsável pela aplicação ou serviço, no caso de aplicações bancárias, o PUK ficaria no poder do Banco.