Digital signatures (overview).

A digital signature is an 'electronic analogue' of the ordinary (handwritten) one.

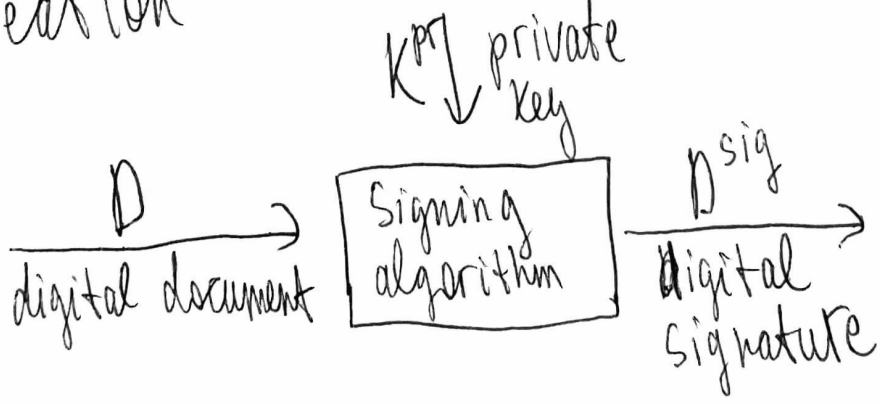
What properties does a signature need to have?

1. Easily verifiable.
2. Very low probability of forgery (very hard to reproduce).

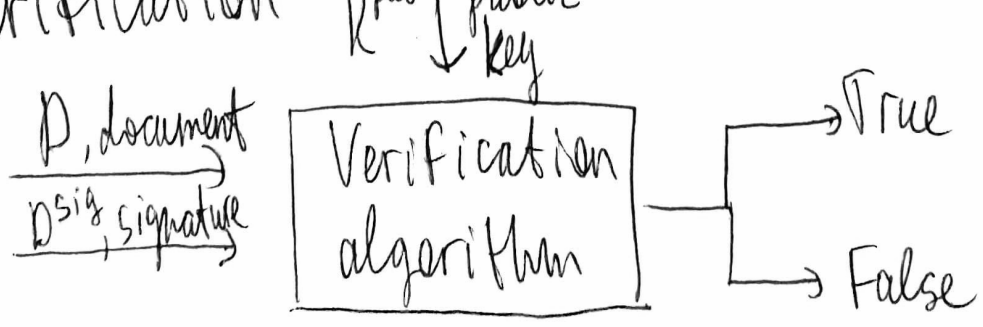
We want the digital signatures to have exactly the same attributes.

Let us give a schematic description of how an electronic signature is created and verified.

1. Creation



2. Verification



Properties we would like to have:

- given K^{pub}, the attacker cannot (feasibly) find K^{pr} or any other number that gives rise to the same signature β^{sig} as K^{pr};
- given K^{pub} and a list of signed documents (and initial ones): $P_1, \dots, P_n, P_1^{sig}, \dots, P_n^{sig}$, the attacker cannot (feasibly) determine P^{sig} for any $P \notin \{P_1, \dots, P_n\}$.

Rmk/def-n. An attack on a digital signature that makes use of a large number of known signatures is called a transcript attack.

Rmk. Most signing algorithms are capable of signing relatively small documents (up to 1000 bits). The solution to this problem is to use a hash function

RSA digital signature.

The idea is very similar to the one underlying RSA cryptosystem. We will use the names Samantha and Victor for the signer and verifier.

Step 1. Samantha picks two large distinct primes p and q. She publishes the number $N = pq$ and a verification exponent v (here v is a number between 1 and $N-1$ with $\gcd(v, (p-1)(q-1)) = 1$.

Samantha's signing exponent (private key) is the number $s \equiv v^{-1} \pmod{(p-1)(q-1)}$.

The signing algorithm is $(s, p) \longmapsto p^s \pmod N$.

Step 2. Victor uses the following verification algorithm:

$$(p, p^s, v) \longrightarrow \begin{cases} \text{true, if } (p^s)^v \equiv p \pmod N \\ \text{false, otherwise.} \end{cases}$$

ElGamal digital signature and Digital Signature Algorithm (DSA)

We start by describing the ElGamal digital signature.

Step 1. Samantha (or a trusted party) chooses a large prime p and a primitive root $g \in \mathbb{F}_p^\times$. Samantha chooses a secret signing exponent s and computes

$$v \equiv g^s \pmod{p}.$$

Her public verification key is the triple (p, g, v).

Step 2. Signing algorithm.

Let $1 < P < p$ be the digital document (number representing it). Samantha chooses a random number $1 < e < p$ and computes

$$S_1 \equiv g^e \pmod{p}$$
$$S_2 \equiv (P - sS_1)e^{-1} \pmod{p-1}.$$

$$(P, e, s, g) \rightsquigarrow (S_1, S_2) \text{ (signature on } P).$$

Step 3. Verification algorithm.

Victor checks the validity of the signature:

$$(P, S_1, S_2, v) \longrightarrow \begin{cases} \text{true}, & v^{S_1} S_1^{S_2} \equiv g^P \pmod{p} \\ \text{false}, & \text{otherwise} \end{cases}$$

Check: $v^{s_1} s_1^{s_2} \equiv g^{sge} \cdot g^{e(p-sge)e^{-1}} \equiv g^{sge+p-sge} \equiv g^p \pmod p$.

Rmk. The pair (s_1, s_2) consists of two numbers, modulo p and $p-1$, thus has length approximately $2\log_2 p$ bits. In order to be secure, p is usually taken between 1000 and 2000 bits.

The Digital Signature Algorithm (DSA) shortens the signature by working in a subgroup of $\mathbb{F}_p^\times$ of prime order q (preserving the level of security).

Step 1. Samantha (or a trusted party) chooses two primes $2^{1000} < p < 2^{2000}$ and $2^{160} < q < 2^{320}$ with $p \equiv 1 \pmod q$, an element $g \in \mathbb{F}_p^\times$ of order q.

Rmk. For instance, if $g' \in \mathbb{F}_p^\times$ is a generator, then $(g')^{\frac{p-1}{q}}$ has order q.

Samantha chooses a secret exponent s and computes

$$v \equiv g^s \pmod p.$$

Verification key: (p, q, g, v).

Step 2. Signature algorithm.

$1 \le p < q$ - digital document

$1 \le e < q$ - ephemeral key

$(D, e, s, q) \longrightarrow (S_1, S_2)$ with

$$S_1 \equiv (g^e \pmod p) \pmod q$$

$$S_2 \equiv (D + sS_1)e^{-1} \pmod q$$

Step 3. Verification algorithm.

Victor computes $V_1 \equiv D S_2^{-1} \pmod q$

$$V_2 \equiv S_1 S_2^{-1} \pmod q$$

$$(g^{V_1} v^{V_2} \pmod p) \pmod q \equiv \begin{cases} S_1, \text{ true} \\ \text{smth else, false.} \end{cases}$$

Check: $g^{V_1} v^{V_2} \equiv g^{D S_2^{-1}} \cdot g^{s S_1 S_2^{-1}} \equiv g^{S_2 S_2^{-1}} \equiv$

$\equiv g^e \pmod p$.

$g^e \equiv S_1 \pmod q$.

The Poisson distribution.

Recall the binomial distribution: we have a random variable X, which takes values $\{0, 1, 2, \ldots, n\}$ with probabilities given by the probability density function (pdf)

$$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Example. Suppose we flip an unfair coin ($p(\text{heads}) = 1/3$ and $p(\text{tails}) = 2/3$) 4 times and let k be the number of heads.

$$P(X=0) = \binom{4}{0} \cdot \left(\frac{2}{3}\right)^4 = \left(\frac{2}{3}\right)^4 = \frac{16}{81}$$

$$P(X=1) = \binom{4}{1} \cdot \left(\frac{1}{3}\right) \cdot \left(\frac{2}{3}\right)^3 = 4 \cdot \frac{1}{3} \cdot \left(\frac{2}{3}\right)^3 = \frac{32}{81}$$

$$P(X=2) = \binom{4}{2} \cdot \left(\frac{1}{3}\right)^2 \cdot \left(\frac{2}{3}\right)^2 = 6 \cdot \left(\frac{1}{3}\right)^2 \cdot \left(\frac{2}{3}\right)^2 = \frac{24}{81}$$

$$P(X=3) = \binom{4}{3} \cdot \left(\frac{1}{3}\right)^3 \cdot \left(\frac{2}{3}\right) = 4 \cdot \left(\frac{1}{3}\right)^3 \cdot \left(\frac{2}{3}\right) = \frac{8}{81}$$

$$P(X=4) = \binom{4}{4} \cdot \left(\frac{1}{3}\right)^4 = \left(\frac{1}{3}\right)^4 = \frac{1}{81}$$

Notice that $\sum_{k=0}^{4} P(X=k) = \frac{16+32+24+8+1}{81} = 1$. This is the defining property of any pdf.

Rmk. How can we show $\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k} = 1$ in general?

Answer: $1 = 1^n = (p+1-p)^n = \sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k}$,

If n and k are large (say, 1000 and 500), the binomial coefficient $\binom{n}{k}$ is hard to compute. Thus we need some easy-to-use approximation. One of the first such approximations was given by Poisson.

Thm (Poisson). Suppose X is a binomial random variable. If $n \to \infty$ and $p \to 0$ in such a way that $\lambda = np$ remains constant, then $\lim_{n\to\infty} P(X=k) = \lim_{n\to\infty} p^k (1-p)^{n-k} \cdot \binom{n}{k} =$

$$= \frac{\lambda^k}{k!} e^{-\lambda}$$

Proof: $\lim_{n\to\infty} \binom{n}{k} p^k (1-p)^{n-k} = \lim_{n\to\infty} \binom{n}{k} \left(\frac{\lambda}{n}\right)^k \left(1-\frac{\lambda}{n}\right)^{n-k} =$

$$= \lim_{n\to\infty} \frac{n!}{k!(n-k)!} \lambda^k \cdot \frac{1}{n^k} \left(1-\frac{\lambda}{n}\right)^{-k} \cdot \left(1-\frac{\lambda}{n}\right)^n = \frac{\lambda^k}{k!} \lim_{n\to\infty} \frac{n!}{(n-k)!} \cdot \frac{1}{(n-\lambda)^k} \left(1-\frac{\lambda}{n}\right)^n$$

Recall that $\lim_{n\to\infty} \left(1-\frac{\lambda}{n}\right)^n = e^{-\lambda}$. It remains to show that $\lim_{n\to\infty} \frac{n!}{(n-k)!} \cdot \frac{1}{(n-\lambda)^k} = 1$.

$\lim_{n\to\infty} \frac{n!}{(n-k)!} \cdot \frac{1}{(n-\lambda)^k} = \lim_{n\to\infty} \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{(n-\lambda)\cdot(n-\lambda)\cdot\ldots\cdot(n-\lambda)} = 1$ (the limit is the ratio of leading coefficients).

Def-n. A random variable X is said to have a Poisson distribution if $P(X=k) = \frac{\lambda^k}{k!} e^{-\lambda}$ with $k \in \mathbb{Z}_{\geq 0} = \{0,1,2,3,\ldots\}$ and $\lambda > 0$ is a constant.

Thm. (1) $P_X(k)$ defines a pdf.

(2) $\mathbb{E}(X) = \lambda$

(3) $\mathrm{Var}(X) = \lambda$.

Proof: (1) clearly $p_X(k) \geq 0 \ \forall k \in \mathbb{Z}_{\geq 0}$ and

$$\sum_{k=0}^{\infty} P_X(k) = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} = e^{-\lambda} \cdot \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} = e^{-\lambda} \cdot e^{\lambda} = 1.$$

(2) let $\frac{\partial}{\partial_x}$ be the differential operator, which acts on functions via taking the derivative with respect to λ, i.e. $\frac{\partial}{\partial_x}(f(\lambda)) = f'(\lambda)$.

By definition $\mathbb{E}(X) = \sum_{k=0}^{\infty} P_X(k) \cdot k = \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda} \cdot k$.

On the other hand, we claim that

$$\mathbb{E}(X) = \left(\lambda \frac{\partial}{\partial_x} + \lambda\right) \left(\sum_{k=0}^{\infty} \frac{\lambda^k}{k!} e^{-\lambda}\right). \quad (\bigstar)$$

Let's check that (☆) holds:

$$\left(\lambda\frac{\partial}{\partial\lambda}+\lambda\right)\left(\frac{\lambda^k}{k!}e^{-\lambda}\right)=\lambda\frac{\partial}{\partial\lambda}\left(\frac{\lambda^k}{k!}e^{-\lambda}\right)+\frac{\lambda^{k+1}}{k!}e^{-\lambda}=$$

$$=\lambda\left(k\cdot\frac{\lambda^{k-1}}{k!}e^{-\lambda}-\frac{\lambda^k}{k!}e^{-\lambda}\right)+\frac{\lambda^{k+1}}{k!}e^{-\lambda}=$$

$$=\frac{\lambda^k}{k!}e^{-\lambda}\cdot(k-1+1)=\frac{\lambda^k}{k!}e^{-\lambda}\cdot k$$

As $\sum_{k=0}^{\infty}\frac{\lambda^k}{k!}e^{-\lambda}=1$ (checked in (1)), (☆) gives

$$\mathbb{E}(X)=\left(\lambda\frac{\partial}{\partial\lambda}+\lambda\right)(1)=0+\lambda=\lambda.$$

Exercise. Show that (3) holds (in similar fashion).

Suppose that a series of events is occuring during a time interval of length T. Divide $[0,T)$ into n subintervals of length $\frac{T}{n}$ (assume n is large). Furthermore, assume that

1. The probability of two or more events occuring in the same subinterval is 0 (in other words, we have a Bernoulli random variable on each subinterval).
2. The probability of occurence in one subinterval is independent of one in any other and is equal to $p=\frac{T}{n}\cdot\lambda$
3. The probability that an event occurs during a subinterval of given length is constant over $[0,T)$

Rmk. (1)-(3) imply that we have a binomial (as sum of Bernoulli) distribution over the interval $[0,T)$ and as $n \to \infty$ this tends to a Poisson distr-n (Thm 1) with mean

$$np = \frac{T}{n} \cdot \lambda \cdot n = \lambda T.$$

Examples.

(1) Suppose a bus arrives every 10 minutes (on average) according to a Poisson process.

(a) Find the probability that there will be 3 buses in the next 15 minutes.

Answer: $\lambda = 1 \text{ bus} / 10 \text{ mins} = 1.5 \text{ buses} / 15 \text{ mins}$.

(property (3))

$$P(X=3) = \frac{(1.5)^3}{3!} e^{-1.5} \approx 0.126$$

(b) Find the probability that you have to wait at least 10 minutes for the next bus.

Answer: take $\lambda = 1 \text{ bus} / 10 \text{ mins}$.

$$P(X=0) = \frac{1^0}{0!} e^{-1} = \frac{1}{e} \approx 0.368$$

(c) Find the probability that at least 3 buses arrive in the next 20 minutes.

Answer: this time take $\lambda = 2$ buses/20 mins

$$P(X \geq 3) = 1 - P(X=0) - P(X=1) - P(X=2) = 1 - e^{-2}\left(1 + \frac{2^1}{1!} + \frac{2^2}{2!}\right) = 1 - 5e^{-2} \approx 0.323.$$

(2) Adding blocks to the bitcoin blockchain. More on that later.