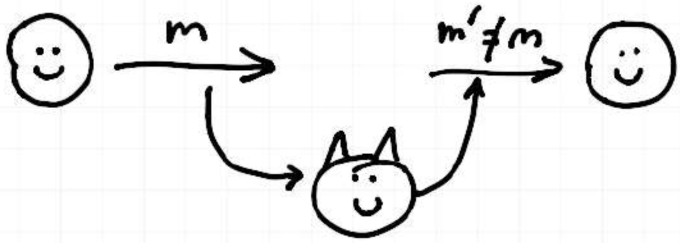
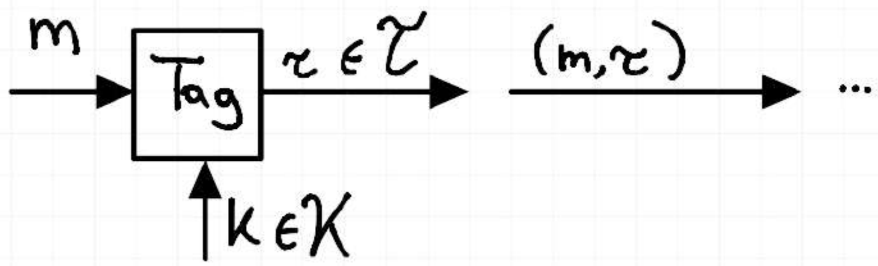
The main question we want to answer is the problem of secure communication and message confidentiality.

Another big problem though is message integrity.
As usual, this is our setup.



The eavesdropper intercepts and changes the message.
How can the receiver know if the message he receives is the same that was sent by the sender?

MESSAGE AUTHENTICATION CODE (MAC)



Tag is an algorithm that "signs" the message, and both m and τ are sent.
The receiver receives the message and the tag, and he accepts it only if he knows the tag is correct. (Bob receives (m, τ'), accepts it if $\tau' = \tau$)

DEF (Perfect MAC)

We say that Tag has one-time ε-statistical security, if $\forall m, m' \in \mathcal{M}, \forall \tau, \tau' \in \mathcal{T}$

$$\Pr[Tag(K, m') = \tau' \mid Tag(K, m) = \tau] \leq \varepsilon$$

the probability that the attacker can force the tag

EX. Show that $\varepsilon = 0$ is impossible

EX. Show that OTP is not secure as a MAC

DEF (Pairwise Independence)

A family of functions

hash functions

$$\mathcal{H} = \{h_K : \mathcal{M} \to \mathcal{T}\}_{K \in \mathcal{K}}$$

is pairwise independent if

$\forall m, m'$ it holds that $\underbrace{(h_K(m), h_K(m'))}^{\text{this is a distribution}}$ is uniform over $\mathcal{T}^2$ for random $K \in \mathcal{K}$

THM: Let $\mathcal{H}$ be pairwise independent and

$Tag(K, m) = h_K(m)$ } if my tag is a hash of the message with the key

Then Tag is $\frac{1}{|\mathcal{T}|}$-statistically secure.

Proof. By pairwise independence

$\forall (m, \tau) \in \mathcal{M} \times \mathcal{T}$

$$\Pr[\mathrm{Tag}(K, m) = \tau] = \Pr[h_K(m) = \tau]$$

$$= \frac{1}{|\mathcal{T}|}$$ ⇒ because by P-I it's uniform

Moreover, $\forall m, m' \in \mathcal{M}, \forall \tau, \tau' \in \mathcal{T}$

$$\Pr[\mathrm{Tag}(K, m) = \tau \wedge \mathrm{Tag}(K, m') = \tau']$$

$$= \Pr[h_K(m) = \tau \wedge h_K(m') = \tau']$$

$$= \frac{1}{|\mathcal{T}|^2}$$ ⇒ the probability is uniform bc the functions are independent

Now, apply BAYES

$\forall m, m' \in \mathcal{M}, \forall \tau, \tau' \in \mathcal{T}$

$$\Pr[\mathrm{Tag}(K, m) = \tau \mid \mathrm{Tag}(K, m') = \tau']$$

$$= \frac{\Pr[\mathrm{Tag}(K, m) = \tau \wedge \mathrm{Tag}(K, m') = \tau']}{\Pr[\mathrm{Tag}(K, m) = \tau]}$$

$$= \frac{1/|\mathcal{T}|^2}{1/|\mathcal{T}|} = \frac{1}{|\mathcal{T}|}.$$

CONSTRUCTION

Let p be a prime. Define

$$h_{a,b}(m) = am + b \mod p$$

$$\mathcal{M} = \mathcal{T} = \underbrace{\mathbb{Z}_p}_{=[0,p-1]} \text{ and } \mathcal{K} = \mathbb{Z}_p^2$$

<u>THM</u>: The above $\mathcal{H} = h_{a,b}$ is pairwise independent

<u>PROOF:</u>

For all $m, m' \in \mathbb{Z}_p$, $\forall \tau, \tau' \in \mathbb{Z}_p$

$$\Pr_{a,b}[h_{a,b}(m) = \tau \wedge h_{a,b}(m') = \tau']$$

$$= \Pr_{a,b}\left[\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau \\ \tau' \end{pmatrix}\right] =$$

$$= \Pr_{a,b}\left[\begin{pmatrix} a \\ b \end{pmatrix} = \underbrace{\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}^{-1}}_{\text{it exists as } m \neq m'}\begin{pmatrix} \tau \\ \tau' \end{pmatrix}\right]$$

$$= 1/p^2$$

LIMITATIONS

1) $|\mathcal{K}| = 2|\mathcal{M}|$ (in $\mathbb{Z}_p$ based contructions because $k = (a,b)$)

2) EX. Define a TWO-TIME variant of STAT.SECURE MAC
Then, show above $\mathbb{Z}_p$-based construction

is not 2-time secure

THM. Any t-TIME $2^{-\lambda}$-STAT-SECURE MAC has key of size $(t+1)\cdot\lambda$

RANDOMNESS EXTRACTION

How does one generate a random key?

VON NEUMANN EXTRACTOR

Suppose B is a biased coin

$$\Pr[B=0] = p < \frac{1}{2}$$

How to get a random coin?

1. sample $b_1 \leftarrow B$, $b_2 \leftarrow B$
2. If $b_1 = b_2$, sample again
3. If $b_1 = 0, b_2 = 1$ output 0
   If $b_1 = 1, b_2 = 0$ output 1

$$\Pr[b_1=0 \wedge b_2=1] = \Pr[b_1=0 \wedge b_2=1] =$$
$$= (1-p)\cdot p \rightarrow \text{uniform!}$$

At each step we output something with probability

$$2p(1-p)$$

After n steps we don't output anything with

$$p \leq (1-2p(1-p))^n$$

In real life we have sources that are unpredictable.
This is measured using MIN-ENTROPY

<u>DEF</u>. The min-entropy of RV X is

$$H_\infty(X) = -\log \max(\Pr[X=x])$$

<u>Example</u>: Take $X \equiv \overset{\to \text{uniform}}{U_m}$ over $\{0,1\}^n$

$$H_\infty(X) = -\log \frac{1}{2^n} = n$$

Take X such that $\Pr[X=0^n]=1$
$\Pr[X \neq 0^n] = 0$

$$H_\infty(X) = -\log 1 = 0 \Rightarrow \text{super predictable}$$
(it's always 0...)

DEF. An (n,k)-source is $X \in \{0,1\}^n$
with $H_\infty(X) \geq k$

GOAL: Exctract uniform randomness from a (n,k)-source

Q: can we have a "magic" function Ext

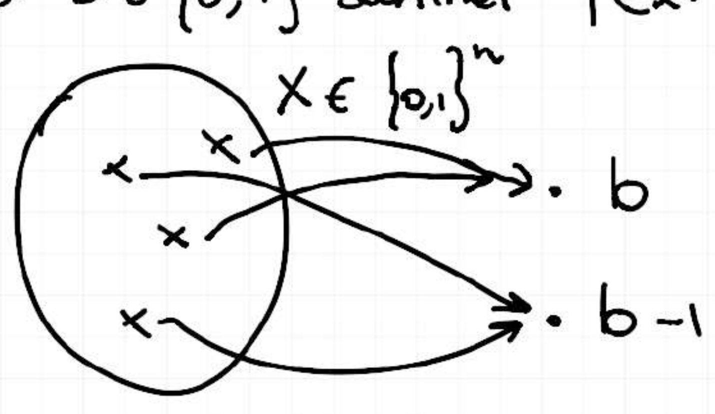
that works $\forall$ n,k-sources X?

A: No. Not even if $Ext: \{0,1\}^n \to \{0,1\}$

and $k = n-1$

Why? Take any $Ext: \{0,1\}^n \to \{0;1\}$

Let $b \in \{0;1\}$ suchthat $|Ext^{-1}(b)| \geq 2^{n-1}$



Define X_{BAD} to be uniform over this $Ext^{-1}(b)$

Now: $Ext(X_{BAD}) = b$ (not random)

and $H_\infty(X_{BAD}) \geq n-1$ (this is really bad for some reason)

So, now what? SEEDED EXTRACTION

We are going to use a series of parametrized extractors that are going to be indexed

DEF. A function $Ext: \underbrace{\{0,1\}^d}_{\text{seed}} \times \underbrace{\{0,1\}^n}_{\text{source}} \to \{0,1\}^\ell$

is a (k,ε)-extractor if

$\forall X \in \{0,1\}^n$ s.t. $H_\infty(X) \geq k$ we have

statistical distance

$$SD\big((S, Ext(S,X)); (S, U_\ell)\big) \leq \varepsilon$$

where U_ℓ is uniform over $\{0,1\}^\ell$

S " " " $\{0,1\}^d$

this means that the extractor is really close to a uniform distribution : want the extractor output to look uniform to the attacker, so really random
This will still not be trivial with a short seed

$$SD(X; X') = \frac{1}{2} \sum_x \left| Pr[X = x] - Pr[X' = x] \right|$$