Msg Auth Codes (MAC)
Hashing
Digital Signatures
Authentication

Alice sends Bob a message $m$ (likely encoded but not our concern)
Authentication

Alice sends Bob a message $m$ (likely encoded but not our concern)
Or does she?
Authentication

Alice sends Bob a message $m$ (likely encoded but not our concern)

Or does she?

Maybe it was send by Eve!
Authentication

Alice sends Bob a message \( m \) (likely encoded but not our concern)
Or does she?
Maybe it was send by Eve!
We need Alice to be able to Authenticate it came from Bob.
Authentication

Alice sends Bob a message \( m \) (likely encoded but not our concern)
Or does she?
Maybe it was send by Eve!
We need Alice to be able to Authenticate it came from Bob.

**Note:** In this lecture we do not care what \( m \) is. It could be a ciphertext and perhaps should be called \( c \). But we call it \( m \). We are only concerned with authentication.
Authentication

Alice sends Bob a message $m$ (likely encoded but not our concern)
Or does she?
Maybe it was send by Eve!
We need Alice to be able to Authenticate it came from Bob.

*Note:* In this lecture we do not care what $m$ is. It could be a ciphertext and perhaps should be called $c$. But we call it $m$. We are only concerned with authentication.

*Terminology:* Security is not the right term. Non-forgeability is. We still use the term Security Parameter.
Formal Def of MAC

Def: A MAC is $\Pi = (GEN, MAC, V)$ where:

1. $GEN(1^n)$ is a uniform $k \in \{0, 1\}^n$.
2. Given key $k$ and msg $m$, $MAC_k(m) = t$, a tag. $MAC_k$ is PPT.
3. $V_k(m, t) = 1$ if $MAC_k(m) = t$, 0 otherwise.

How to Use: Alice and Bob have $\Pi = (GEN, MAC, V)$

1. Alice generates $k$ via $GEN$ and sends it to Bob privately.
2. To send $m \in \{0, 1\}^*$ to Alice, Bob computes $t = MAC_k(m)$ and sends $(m, t)$.
3. Alice authenticates that its from Bob iff $V_k(m, t) = 1$.

Note: We often restrict to $m \in \{0, 1\}^{p(n)}$, $p$ poly.
Example of a MAC

1. \(k \in \{0, \ldots, p - 1\}\) unif.
2. \(MAC_k(m) = m + k\).
3. \(V_k(m, t) = 1\) if \(t = m + k\)

Not Secure: If Eve has access to \(MAC_k\) or has old messages she knows \(k = 7\).
Eve can Forge: If Eve has key \(k\) then she can forge.
Example of a MAC

1. \( k \in \{0, 1\}^n \) unif.
2. \( MAC_k(m) = m \oplus k \).
3. \( V_k(m, t) = 1 \) if \( t = m \oplus k \)

Not Secure: If Eve has access to \( MAC_k \) or has old messages she knows \( k \).

Eve can Forge: If Eve has key \( k \) then she can forge.

Need: A function \( f \) such that knowing \( f \) on a few values does not reveal what \( f \) is.
Example of a MAC

1. $k \in \{0, 1\}^n$ unif.
2. $MAC_k(m) = m \oplus k$.
3. $V_k(m, t) = 1$ if $t = m \oplus k$

Not Secure: If Eve has access to $MAC_k$ or has old messages she knows $k$.

Eve can Forge: If Eve has key $k$ then she can forge.

Need: A function $f$ such that knowing $f$ on a few values does not reveal what $f$ is.

We have them! Pseudo-Random Functions!
Construction of a Fixed Length MAC

Message are of length $n$
Let $F$ be a PRF from $\{0, 1\}^n$ to $\{0, 1\}^n$.

MAC:
1. $GEN$: choose a uniform key $k \in \{0, 1\}^n$ for $F$
2. $MAC_k(m)$: output $F_k(m)$
3. $V_k(m, t)$: output 1 iff $F_k(m) = t$

Theorem: $\Pi$ is a non-forgeable MAC
Proof Sketch: If forgeable then $F_k$ would not be pseudorandom.
Issue: We have not defined forgeable formally and we won’t.
Drawbacks?

- This only works for *fixed-length* messages
- Since need tag $t$ to be short, this only works for *short* messages

To get variable length we need a new Hardness Assumption.
Collision Resistant Hash Functions (CRHF)

Informal Def: A function $H$ from $\{0, 1\}^n$ to $X$ where $X$ is finite is Collision Resistant if it is HARD to find $x, y$ such that $H(x) = H(y)$.

Common HA: CRHF
Often keyed: $H_k$ where $k$ is a key. $k$ of length $n$ gives $H$ on $\{0, 1\}^n$. 
**Random Oracle Model (ROM)**

**Def:** The Random Oracle Model is the HS that there exists a CRHF $H$ such that $H$ is indistinguishable from a random function.

**Common HA:** ROM

**Often keyed:** $H_k$ where $k$ is a key.
Random Oracle Model: Warning

Compare the following HA:

- Factoring is hard. Well tested. Fermat (1600’s) worked on it! If Eve can factor 100-bit numbers then goto 200-bits.
- RSA assumption. Worked on since 1978. But 40 years of modern math is a lot. If Eve can crack RSA with 100-bit primes then goto 200 bits.
- ROM. Hmmm. No candidate for the RO has been that well tested. The assumption $H$ is random harder to test then Factoring is hard

But! There are real functions (in two slides) that are really being used that seem to satisfy ROM.
Possible CRHF

Security Parameter $n$

$H_k(x, y)$: $k$ encodes $(p, g, h)$ where

- $p$ is an $n$-bit primes (who would have guessed! :-))
- $g$ is a generator for $\mathbb{Z}_p$
- $h$ is some other random element of $\mathbb{Z}_p$.

$H : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is defined by

$$H(x, y) = g^x h^y \pmod{p}$$

**Note:** This is fixed length, but an use bigger and bigger security parameters so considered to be a function on $\{0, 1\}^n$. 
More CRHF

The following are really used! The definitions are ugly (like Trivium).

<table>
<thead>
<tr>
<th>Hash Sch</th>
<th>Year</th>
<th>Const</th>
<th>Numb bits</th>
<th>Year</th>
<th>Broken</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD4</td>
<td>1990</td>
<td>128</td>
<td></td>
<td>1995</td>
<td></td>
</tr>
<tr>
<td>MD5</td>
<td>1992</td>
<td>128</td>
<td></td>
<td>1998</td>
<td></td>
</tr>
<tr>
<td>SHA1</td>
<td>1994</td>
<td>160</td>
<td></td>
<td>2005*</td>
<td></td>
</tr>
<tr>
<td>SHA-256</td>
<td>2005</td>
<td>256</td>
<td></td>
<td>Not Yet!</td>
<td></td>
</tr>
</tbody>
</table>

*SHA1 – collision found, but not quite broken.
Construction of a $\geq n$-length MAC

Message are of length $\geq n$
Let $F_k$ be a PRF from $\{0, 1\}^n$ to $\{0, 1\}^n$.
Let $H_k$ be a CRHF from $\{0, 1\}^*$ to $\{0, 1\}^n$.
Both keys are in $\{0, 1\}^n$.
MAC:

1. $GEN$: choose a uniform key $k \in \{0, 1\}^n$ for $F$ and $H$
2. $MAC_k(m)$: output $F_k(H_k(m))$
3. $V_k(m, t)$: output 1 iff $F_k(H_k(m)) = t$

Theorem: $\Pi$ is a non-forgeable MAC
Proof Sketch: If forgeable then $F_k$ would not be psuedorandom OR $H_k$ would not be CRHF.
Issue: We have not defined forgeable formally and we won't.
Drawbacks?

Alice: Bob, you signed a document saying you owe me $100,000

Bob: I didn’t! And even if I did you can’t prove it!

Need for the signature to be public!
Digital Signatures
Digital signatures

1. MAC uses private Key
2. MAC is good if Alice and Bob’s only enemy is Eve.
3. MAC is bad if Bob says I didn’t send that

Need a public key version of MAC that witnesses can verify.
Comparison to MACs?

- **Public verifiability**
  - “Anyone” can verify a signature
  - (Only a holder of the key can verify a MAC tag)

- **Transferable**
  - Can forward a signature to someone else . . .

- **Non-repudiation** Bob can’t deny he signed!
Signature schemes

- A signature scheme is defined by three PPT algorithms (GEN, SIGN, V):
  - GEN: takes as input $1^n$, outputs $sk, pk \in \{0, 1\}^n$ (Secret Key, Public Key).
  - SIGN: takes as input a private key $sk$ and a message $m \in \{0, 1\}^*$; outputs a signature $\sigma$
    \[
    \sigma \leftarrow \text{SIGN}_{sk}(m)
    \]
  - V: takes a public key $pk$, message $m$, and signature $\sigma$ as input; outputs 1 or 0
    \[
    \forall m, pk, sk[V_{pk}(m, \text{SIGN}_{sk}(m)) = 1]
    \]
First Attempt at a Signature schemes

1. GEN generates primes \( p, q \) of length \( n \). \( p, q \) is private, \( N = pq \) is public. Let \( R = (p - 1)(q - 1) \). \( e, d \) such that \( ed \equiv 1 \pmod{R} \). \( e \) public, \( d \) private.

2. For Bob to sign message \( m \), Bob sends \( \sigma = m^d \pmod{N} \).

3. To verify Alice computes \( \sigma^d \)

\[
\sigma^e \equiv (m^d)^e \equiv m^{ed} \equiv m^{ed} \pmod{R} \equiv m \pmod{N}.
\]
Looks Secure But Its Not

There are attacks on it that work.

Omitted.

But what to do?

Just a small adjustment.
Second Attempt at a Signature schemes

Assume the Random Oracle Model. Assume Let $H$ be a Random Oracle.

1. $GEN$ generates primes $p, q$ of length $n$. $p, q$ is private, $N = pq$ is public. Let $R = (p - 1)(q - 1)$. $e, d$ such that $ed \equiv 1 \pmod{R}$. $e$ public, $d$ private.

2. For Bob to sign message $m$, Bob sends $\sigma = H(m)^d \pmod{N}$.

3. To verify Alice computes $\sigma^e$:

$$\sigma^e \equiv (H(m)^e)^d \equiv H(m)^{ed} \equiv H(m)^{ed} \pmod{R} \equiv H(m) \pmod{N}.$$ 

Secure?
Second Attempt at a Signature schemes

Assume the Random Oracle Model. Assume Let $H$ be a Random Oracle.

1. $GEN$ generates primes $p, q$ of length $n$. $p, q$ is private, $N = pq$ is public. Let $R = (p-1)(q-1)$. $e, d$ such that $ed \equiv 1 \pmod{R}$. $e$ public, $d$ private.

2. For Bob to sign message $m$, Bob sends $\sigma = H(m)^d \pmod{N}$.

3. To verify Alice computes $\sigma^e$:

\[
\sigma^e \equiv (H(m)^e)^d \equiv H(m)^{ed} \equiv H(m)^{ed} \pmod{R} \equiv H(m) \pmod{N}.
\]

Secure?

Theorem: If a message can be forged then $H$ is not a Random Oracle.
Second Attempt at a Signature schemes

Assume the Random Oracle Model. Assume Let $H$ be a Random Oracle.

1. $\text{GEN}$ generates primes $p, q$ of length $n$. $p, q$ is private, $N = pq$ is public. Let $R = (p - 1)(q - 1)$. $e, d$ such that $ed \equiv 1 \pmod{R}$. $e$ public, $d$ private.

2. For Bob to sign message $m$, Bob sends $\sigma = H(m)^d \pmod{N}$.

3. To verify Alice computes $\sigma^e$:

$$\sigma^e \equiv (H(m)^e)^d \equiv H(m)^{ed} \equiv H(m)^{ed} \pmod{R} \equiv H(m) \pmod{N}.$$ 

Secure?

Theorem: If a message can be forged then $H$ is not a Random Oracle.

Secure!