proof space

Secure…
Cryptographic Time-Stamps

Through Transient Key Technology

By: Paul Doyle of ProofSpace

proof space

We Will Describe A System That…

- Is a method of self-validating proof of time
- Creates Cryptographic Timestamps that never expire
- Is a fully distributed system
- Is immune from the compromise of secret keys
- Is independent of a Trusted Third Party
- Creates a network of validation & verification

The ProofMark System™ Can Be Used To Prove Integrity And Time Existence…

Original Data

…010001100...

...For Any Set Of Data

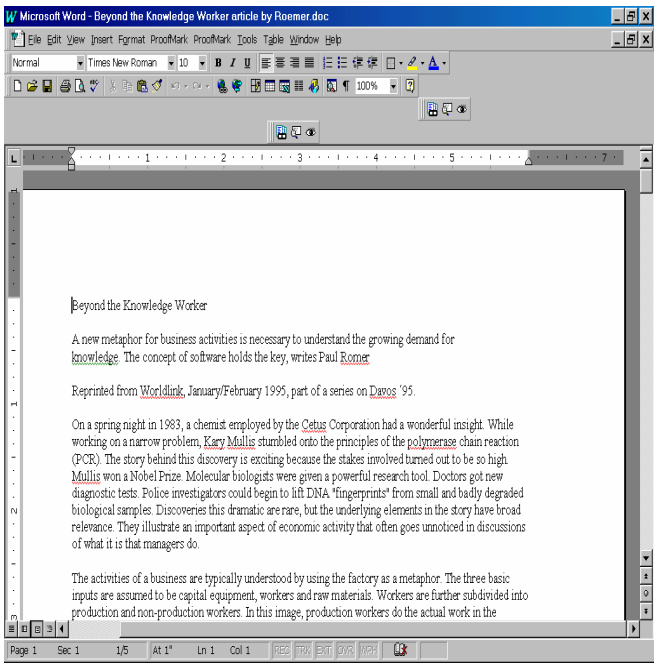
…Or Any Record

Regardless Of The Application…We Can Enable You To Create And Maintain Proof

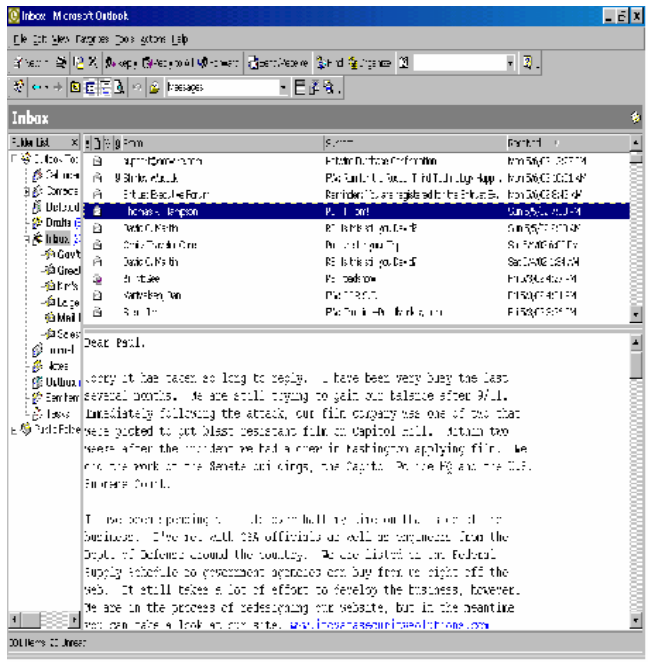
…010001100...

OR

…110001101...

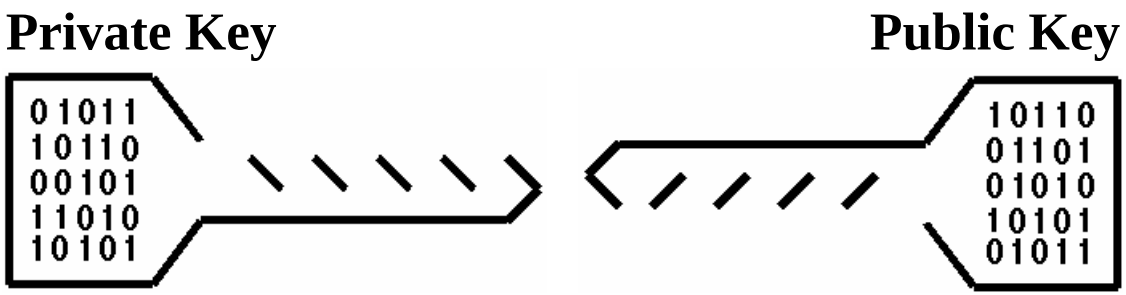


OR

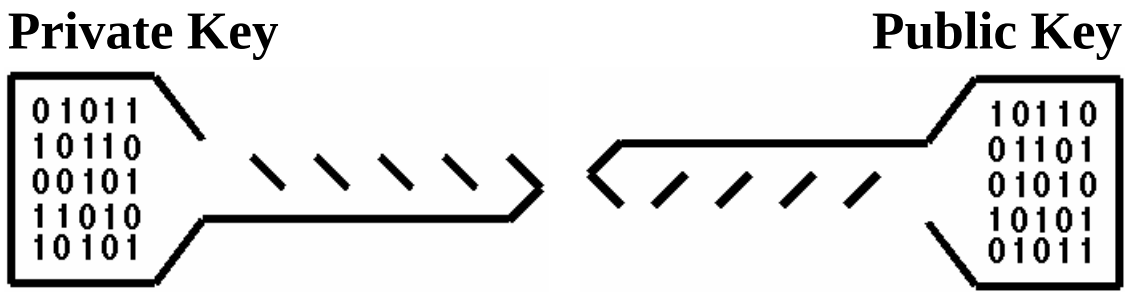


We use asymmetric cryptography…

…but we use it in a new way.

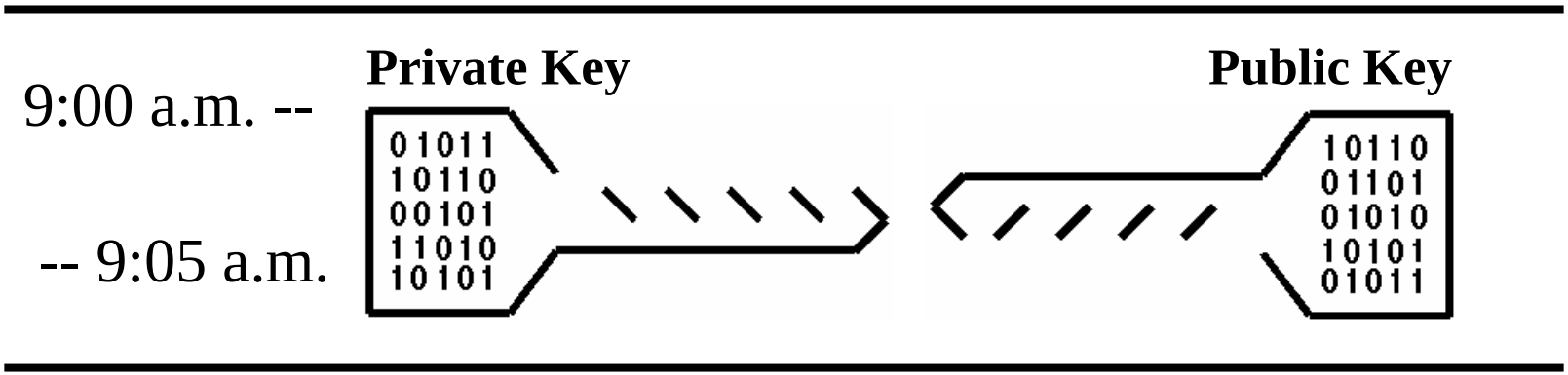


Rather than issuing the Private/Public Key pair to an organization or individual…



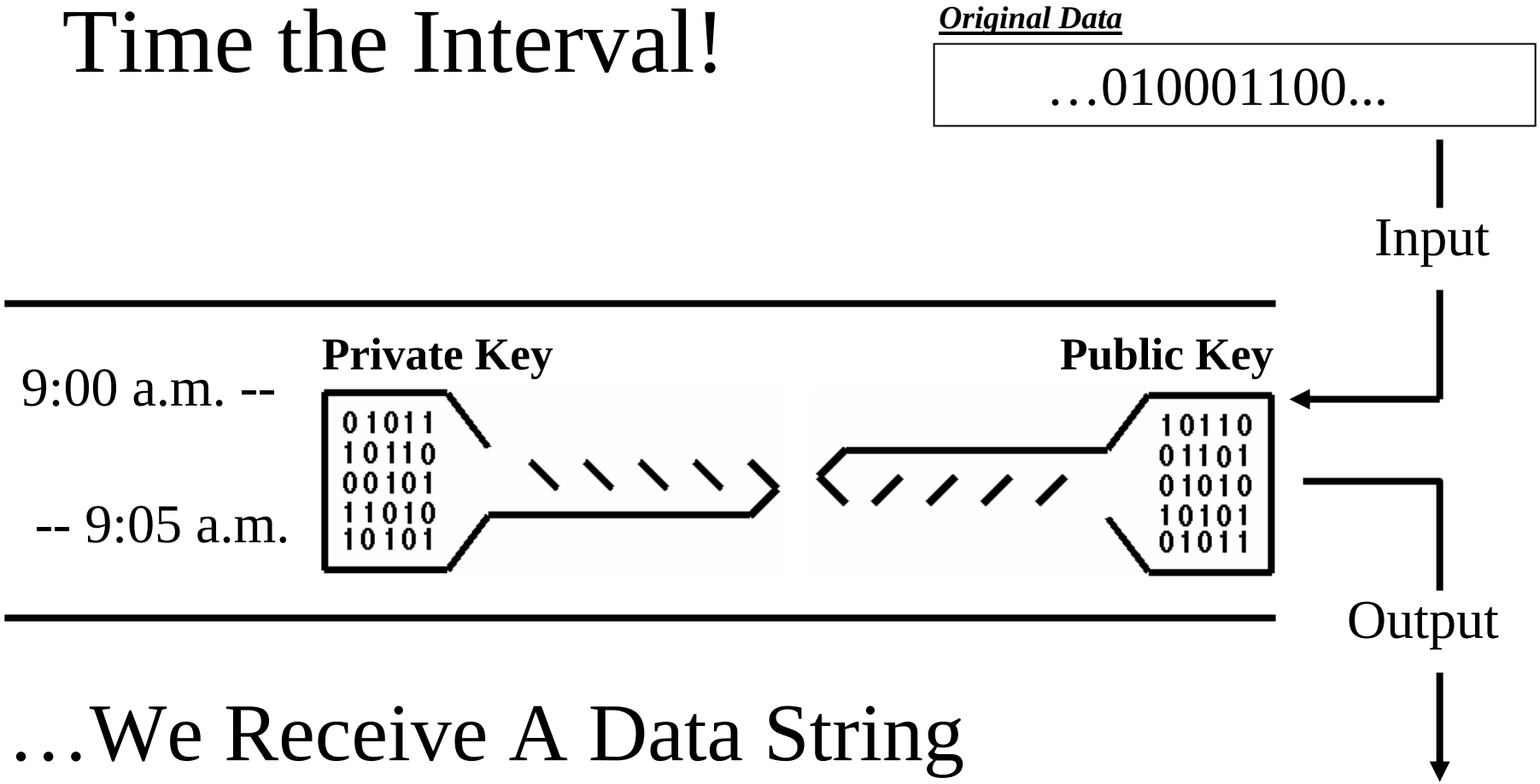
…We issue them to Time!

Not Time the continuum…



…Time the Interval!

Time the Interval!



…We Receive A Data String

…And We Return A Data String

proof space

The ProofMark Certificate Contains Three Critical Elements

Original Data

…010001100...

Output

…10010...

ProofMark Certificate

1.) Original Data

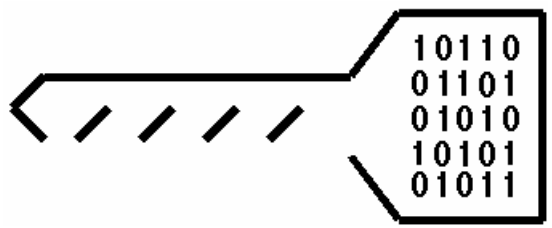
…010001100...

2.) Signature on data from Private Key

X35GJLA92XA!A69...

3.) Time Interval's Public Key

Public Key



proof space

ProofMark Certificate

1.) Original Data

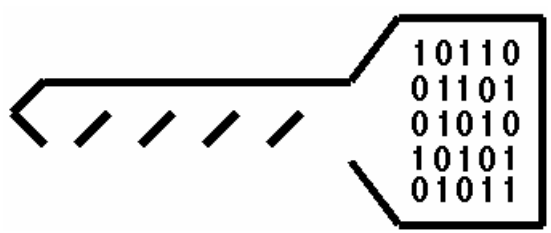
…010001100...

2.) Signature on data from Private Key

X35GJLA92XA!A69...

3.) Time Interval's Public Key

Public Key

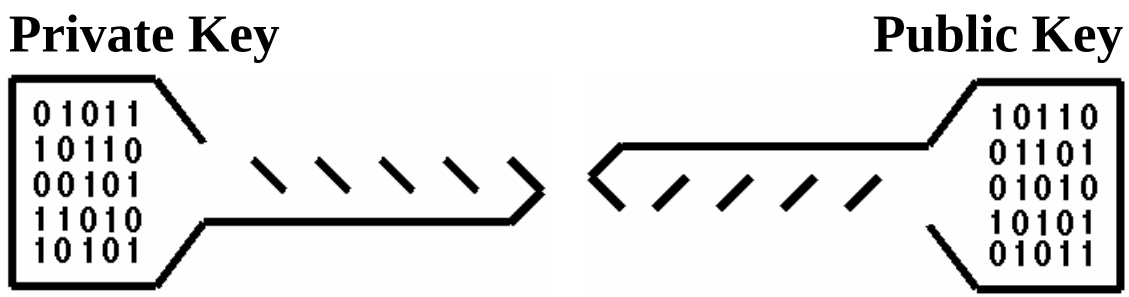


If the Public Key applied to the Signature Resolves to the Original Data…then there is mathematical integrity self-contained within the output!

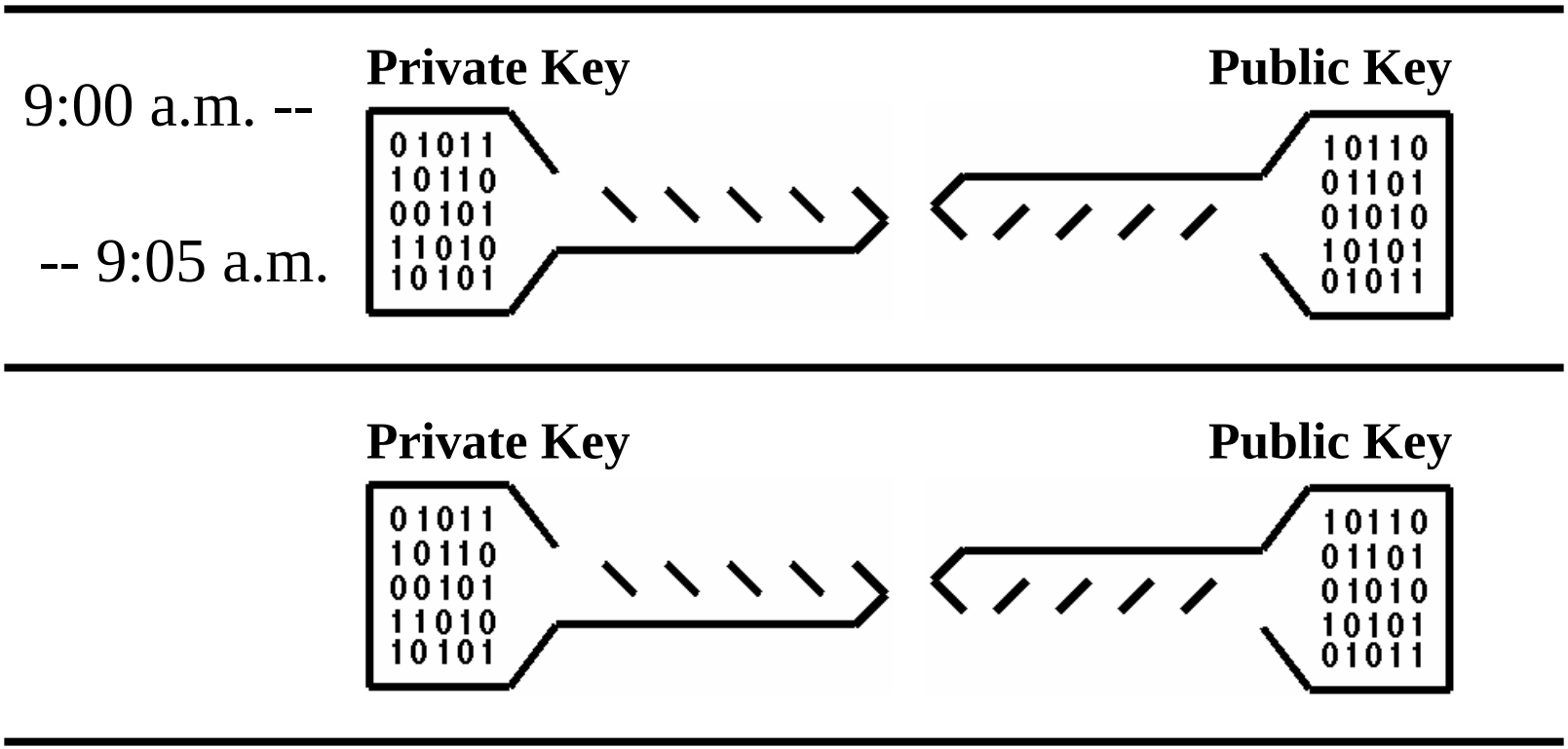
Now, Back to the Server...

9:00 a.m. --

-- 9:05 a.m.

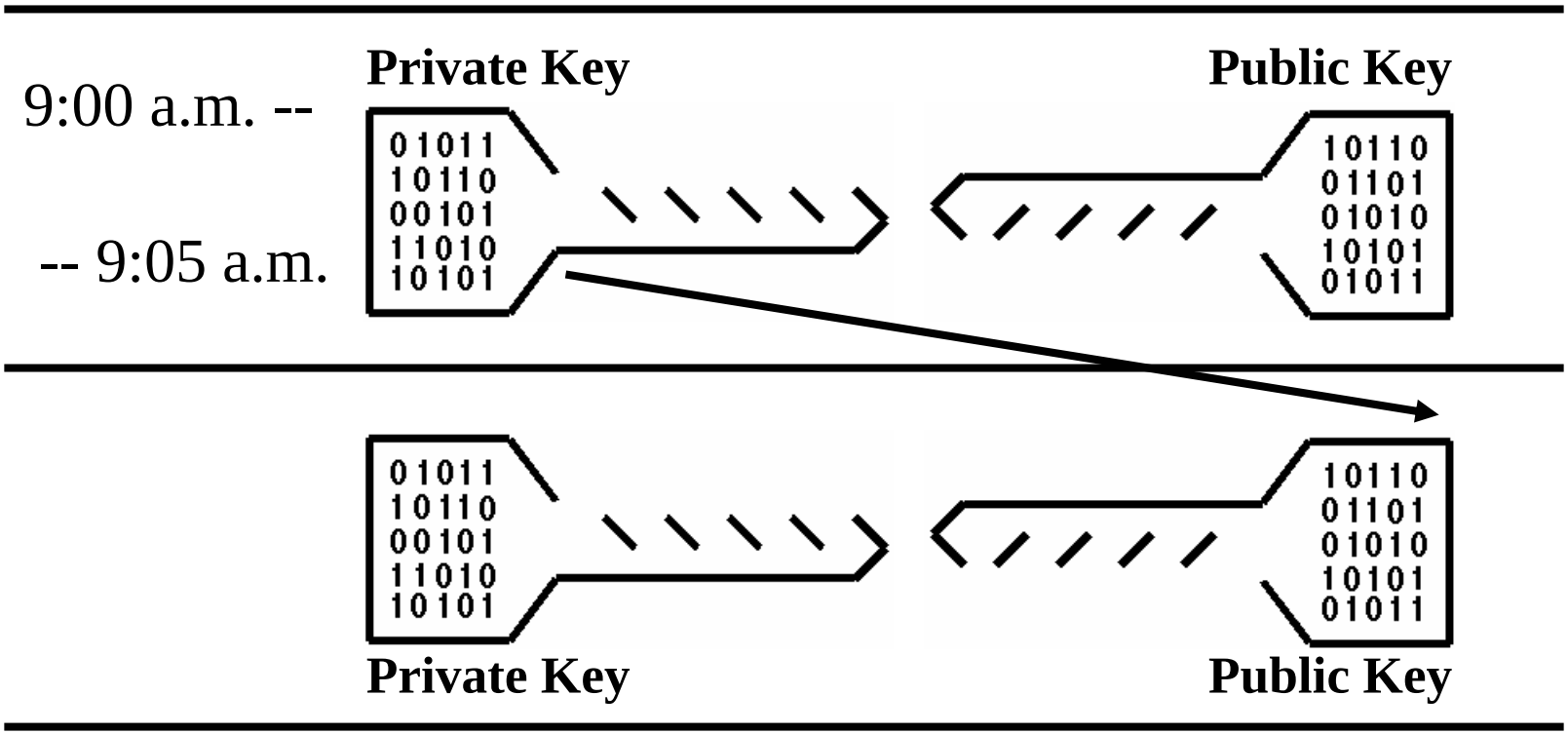


The Last Thing that Happens During the Interval...

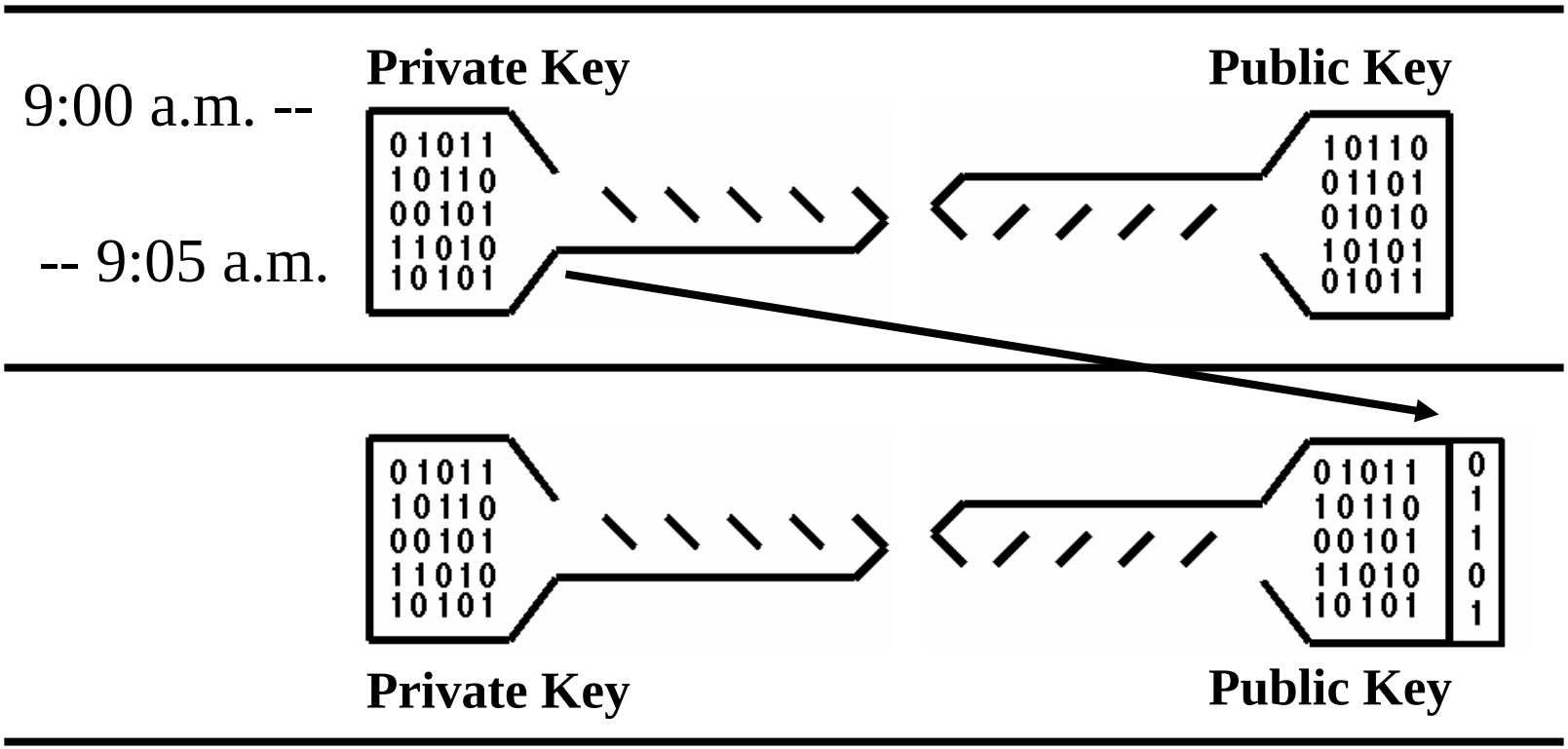


…Is that Independently a New Pair of Keys is Generated.

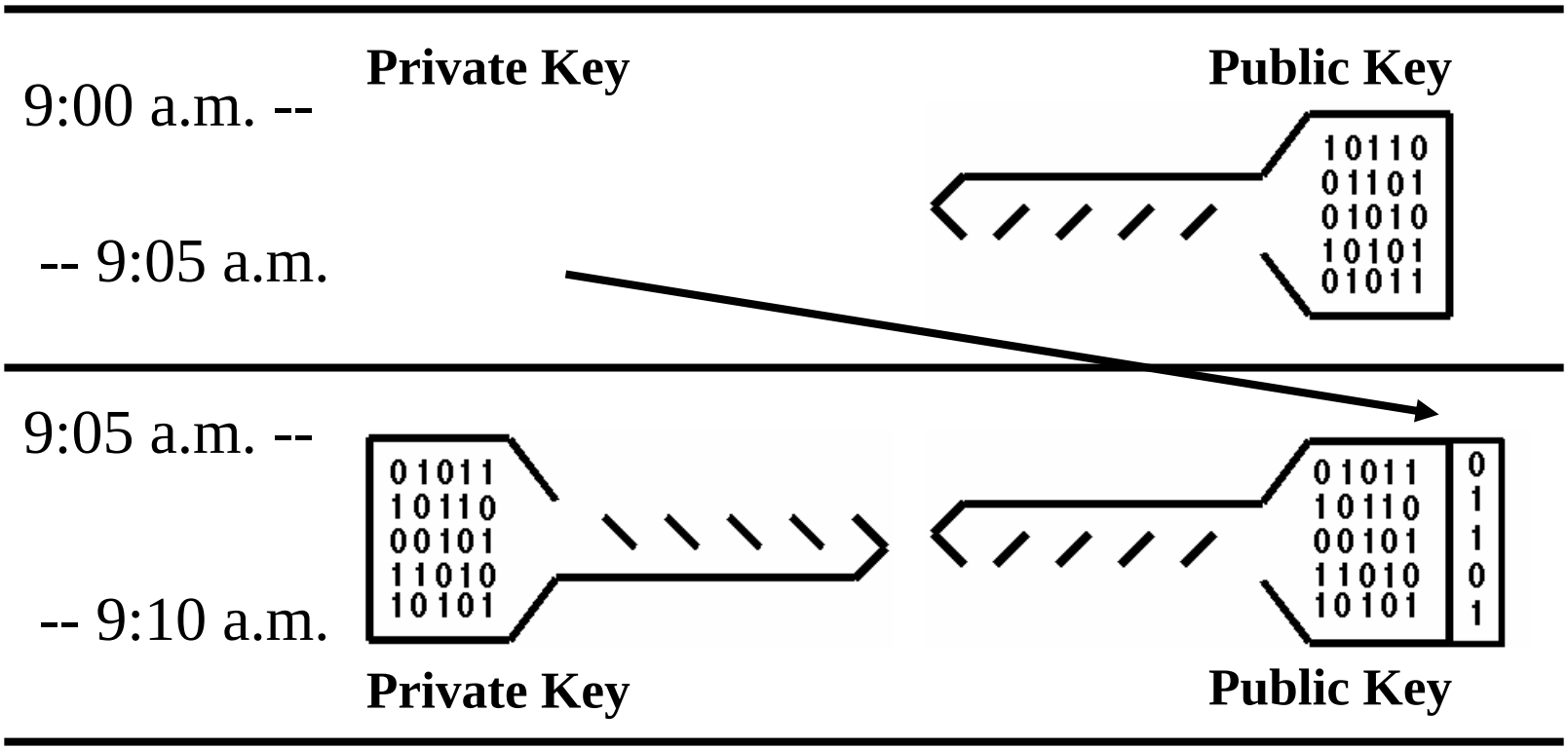
The Current Private Key Signs the New Public Key



Signature on New Public Key Created

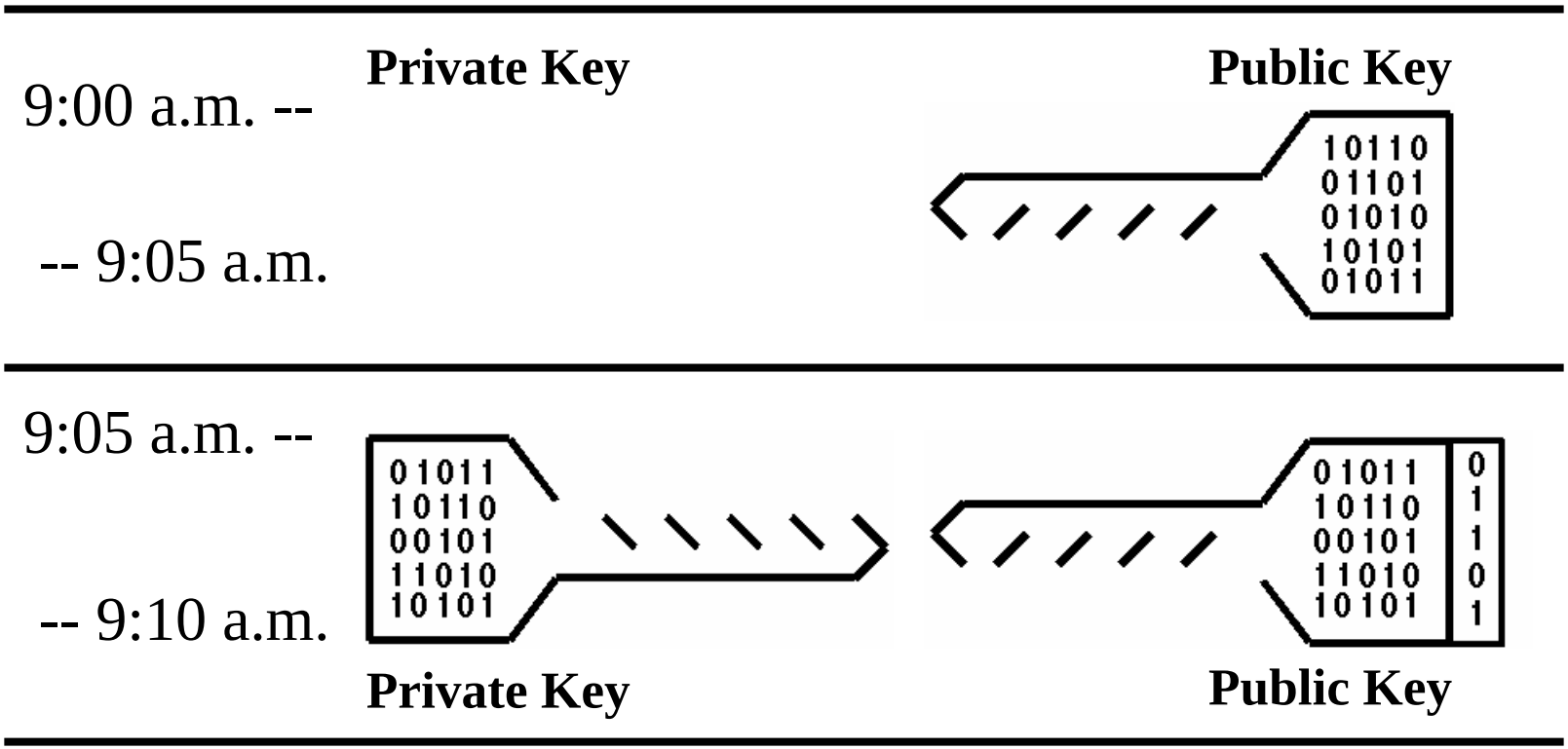


And the Old Private Key Is Destroyed...

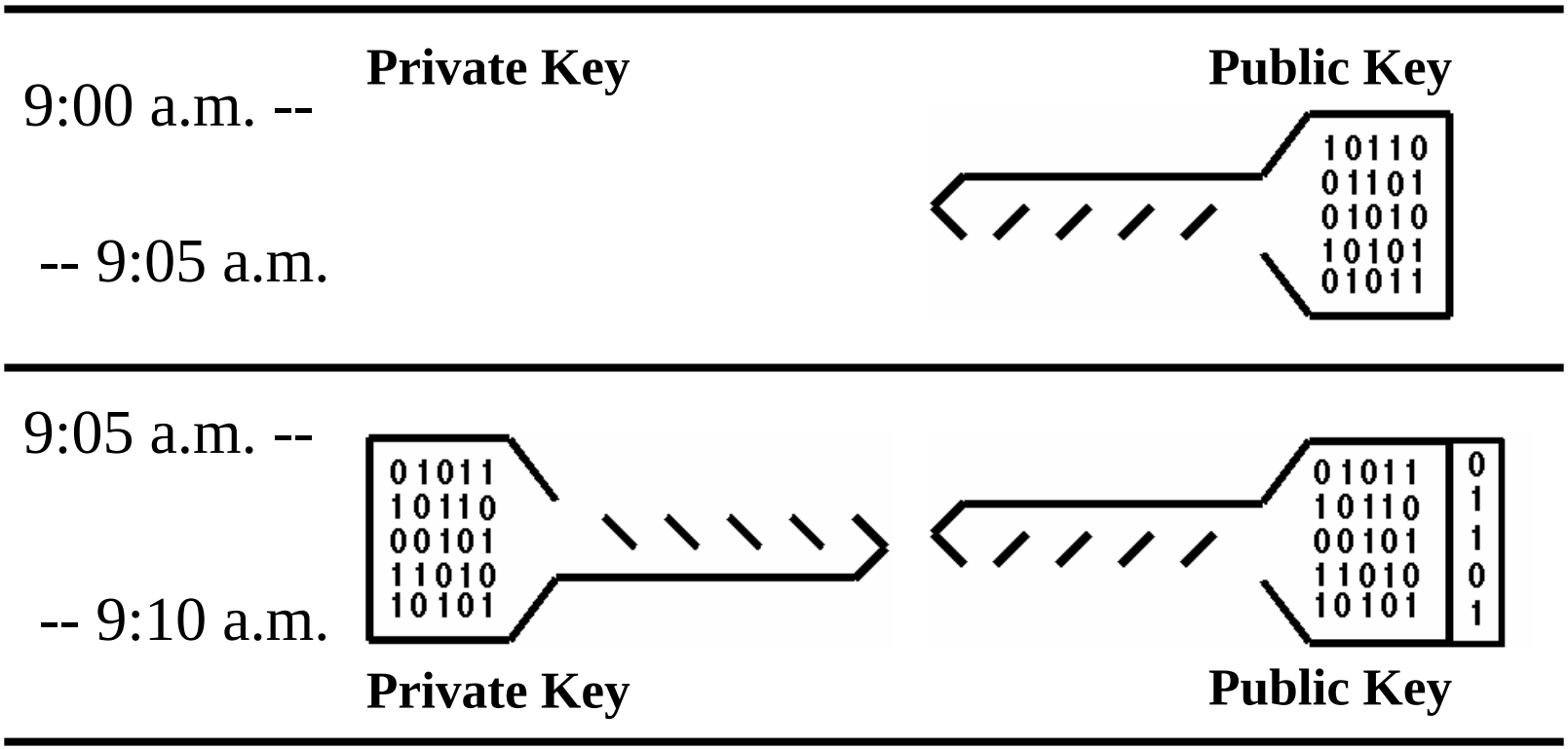


…And the New Key Pair Goes On Duty!

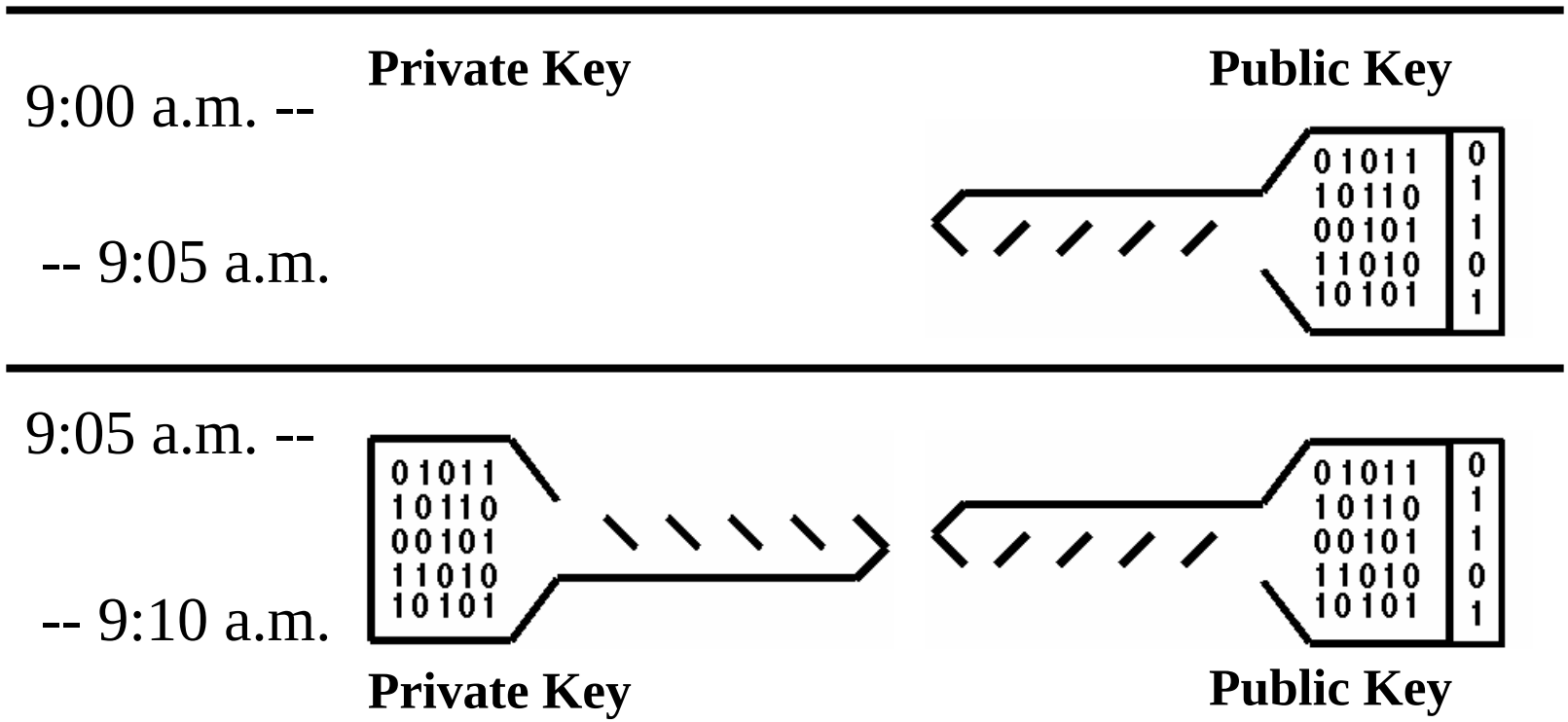
So What You Have ‘After-the-Fact’ For Any Interval Of Time Is Its Public Key...



So What You Have ‘After-the-Fact’ For Any Interval Of Time Is Its Public Key...



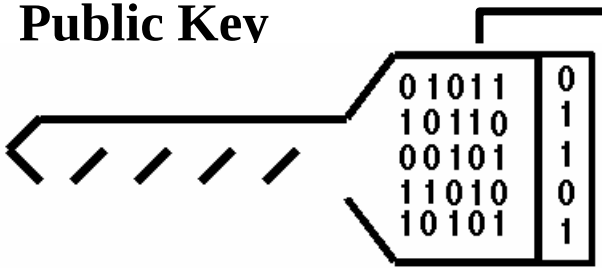
And A Signature On That Key From The Previous Private Key…



...Which No Longer Exists, But For Which You Have The Public Key

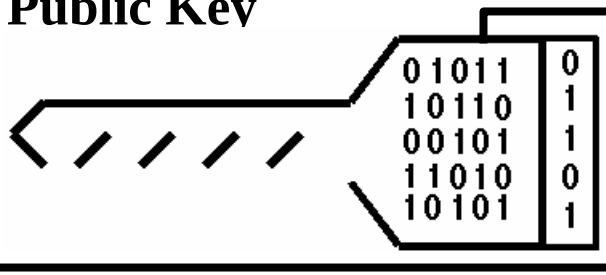
8:50 a.m. --
-- 8:55 a.m.

Public Kev



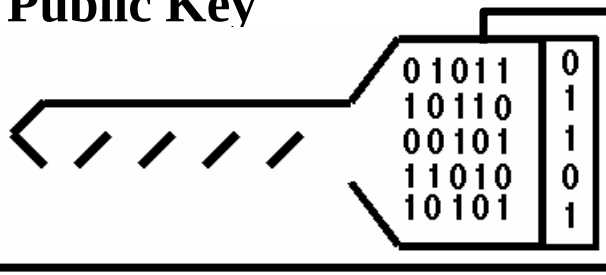
8:55 a.m. --
-- 9:00 a.m.

Public Kev



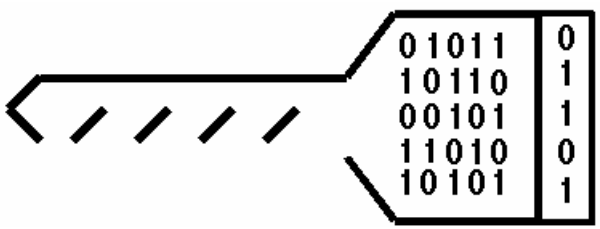
9:00 a.m. --
-- 9:05 a.m.

Public Key



9:05 a.m. --
-- 9:10 a.m.

Public Key

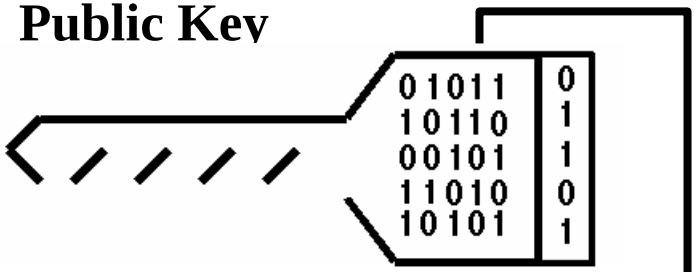


Prior Public Key Verifies Signature On New Public Key

Prior Public Key Verifies Signature On New Public Key

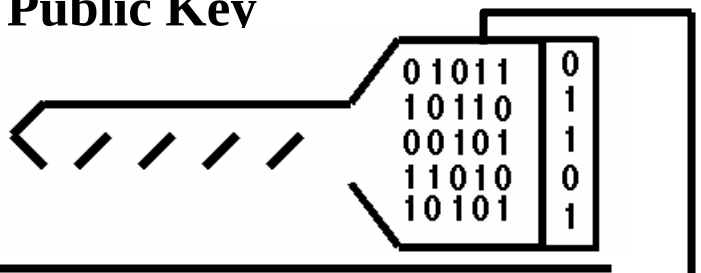
8:50 a.m. --
-- 8:55 a.m.

Public Key



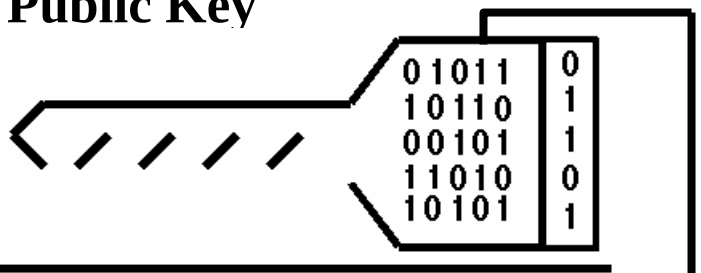
8:55 a.m. --
-- 9:00 a.m.

Public Key



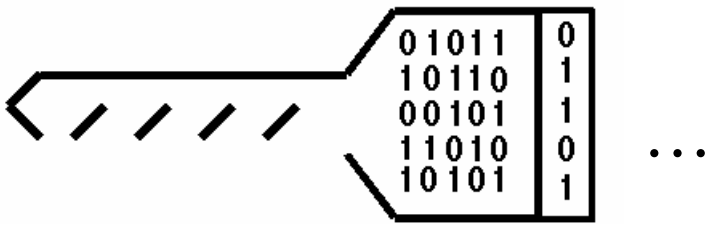
9:00 a.m. --
-- 9:05 a.m.

Public Key



9:05 a.m. --
-- 9:10 a.m.

Public Key

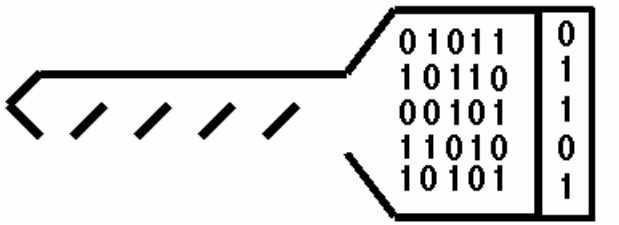


So We Form A Cryptographically Strong Chain Of Public Keys Going Back Through Time…

…Corresponding To Time!!

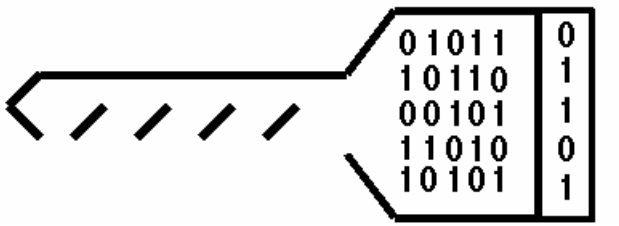
8:50 a.m. -- -- 8:55 a.m.

Public Key



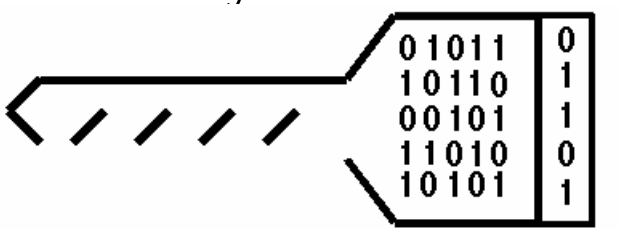
8:55 a.m. -- -- 9:00 a.m.

Public Key



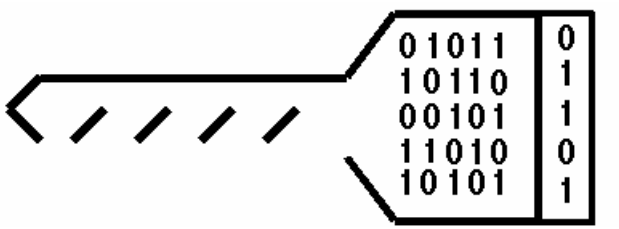
9:00 a.m. -- -- 9:05 a.m.

Public Key



9:05 a.m. -- -- 9:10 a.m.

Public Key



So, There Are No Secrets To Protect…

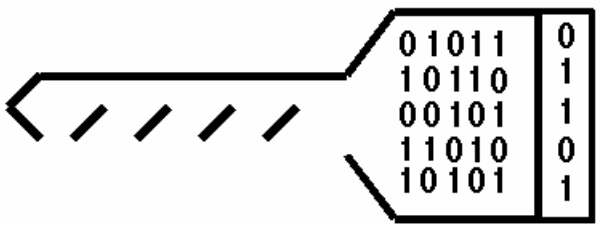
…Because there are No Secrets, We Can Take The Record Of Public Keys And Push Them Out For Public Access...

…In Fact We Can Make Them Part Of The Public Record.

proof space

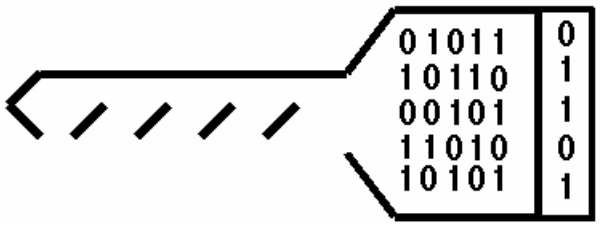
8:50 a.m. --
-- 8:55 a.m.

Public Key



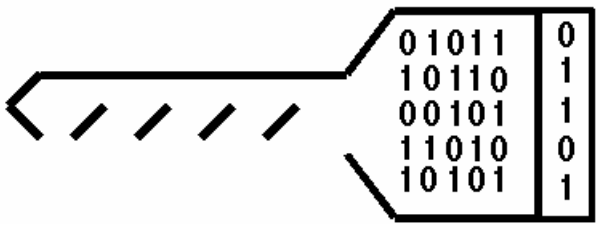
8:55 a.m. --
-- 9:00 a.m.

Public Key



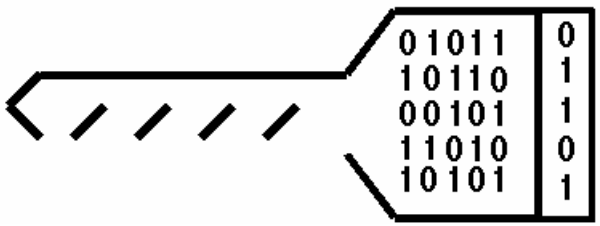
9:00 a.m. --
-- 9:05 a.m.

Public Key



9:05 a.m. --
-- 9:10 a.m.

Public Key



If You Then Take The ProofMark Certificate...

ProofMark Certificate

1.) Original Data

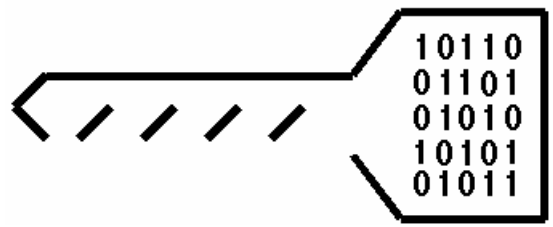
…010001100...

2.) Signature on data from Private Key

X35GJLA92XA!A69...

3.) Time Interval's Public Key

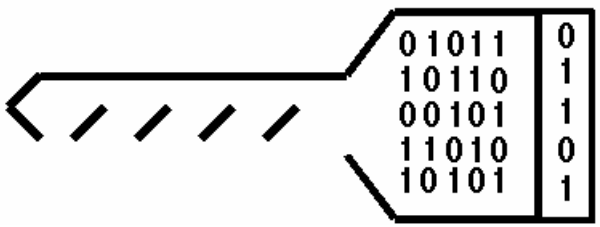
Public Key



proof space

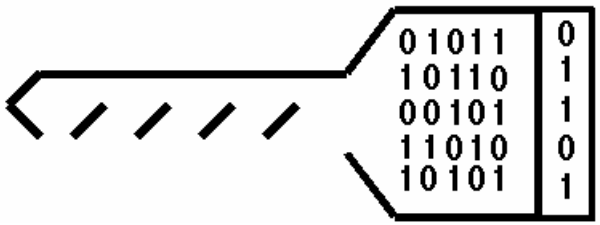
8:50 a.m. --
-- 8:55 a.m.

Public Key



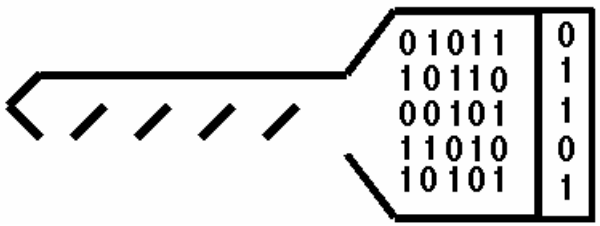
8:55 a.m. --
-- 9:00 a.m.

Public Key



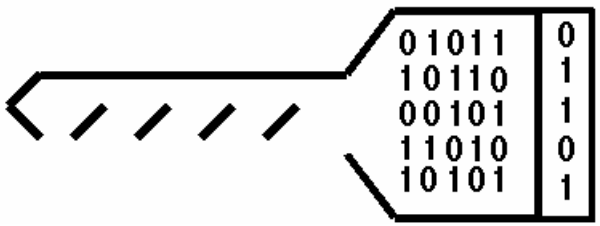
9:00 a.m. --
-- 9:05 a.m.

Public Key



9:05 a.m. --
-- 9:10 a.m.

Public Key



And Compare the Public Key to the Public Key in the Chain

ProofMark Certificate

1.) Original Data

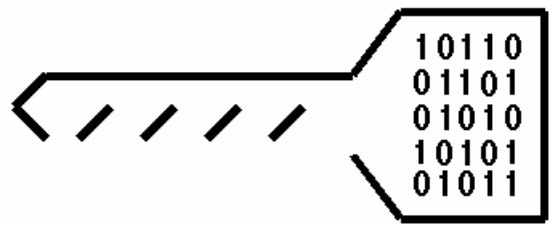
…010001100...

2.) Signature on data from Private Key

X35GJLA92XA!A69...

3.) Time Interval's Public Key

Public Key

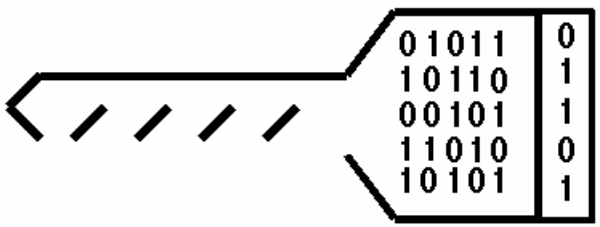


proof space

8:50 a.m. --

-- 8:55 a.m.

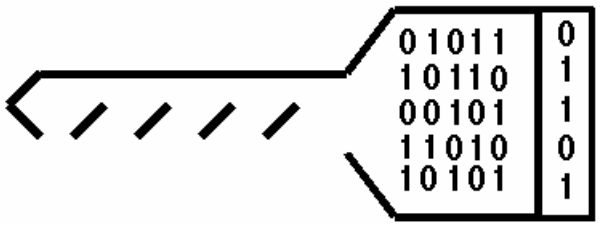
Public Key



8:55 a.m. --

-- 9:00 a.m.

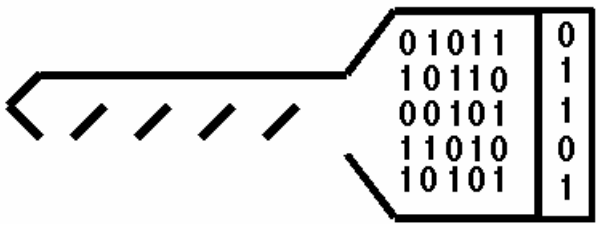
Public Key



9:00 a.m. --

-- 9:05 a.m.

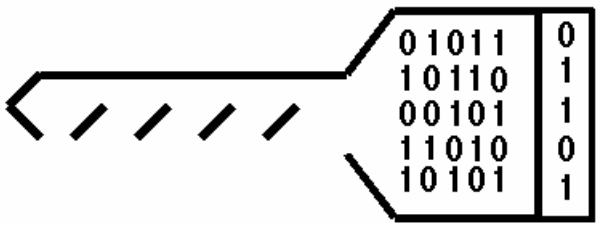
Public Key



9:05 a.m. --

-- 9:10 a.m.

Public Key



If The Keys Are The Same, Then You Have Proof Of Time!

ProofMark Certificate

1.) Original Data

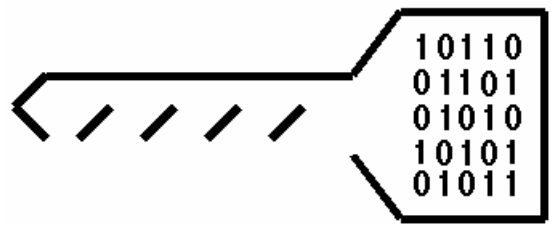
…010001100...

2.) Signature on data from Private Key

X35GJLA92XA!A69...

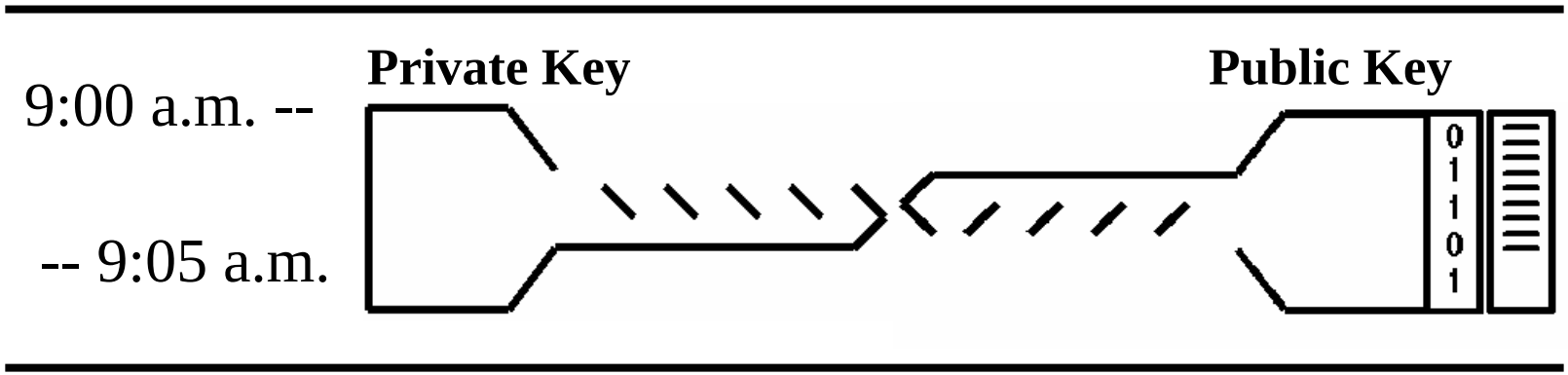
3.) Time Interval's Public Key

Public Key

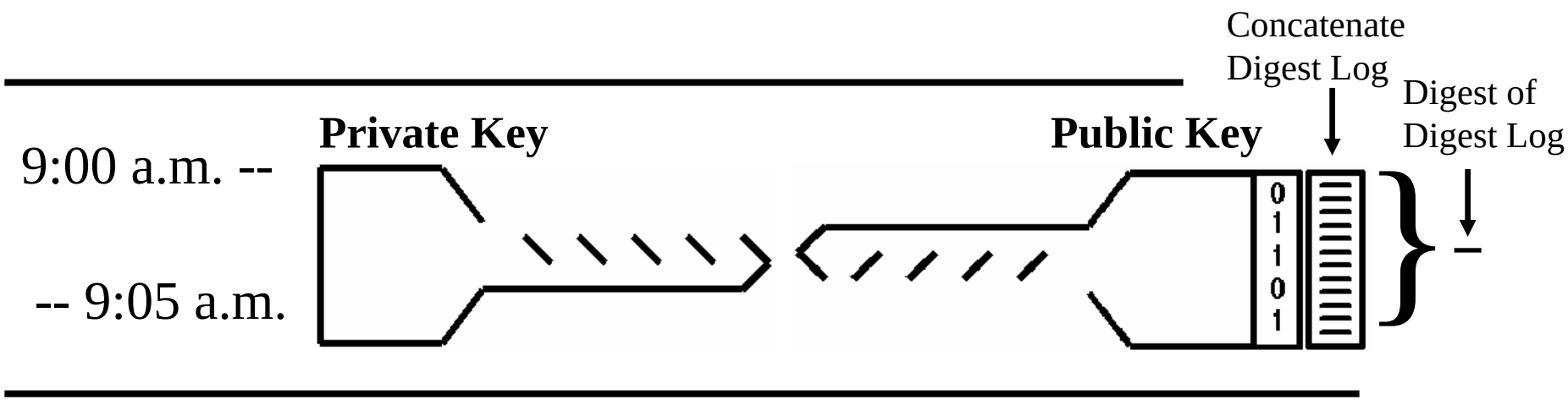


To further protect against the future compromise of a private key…

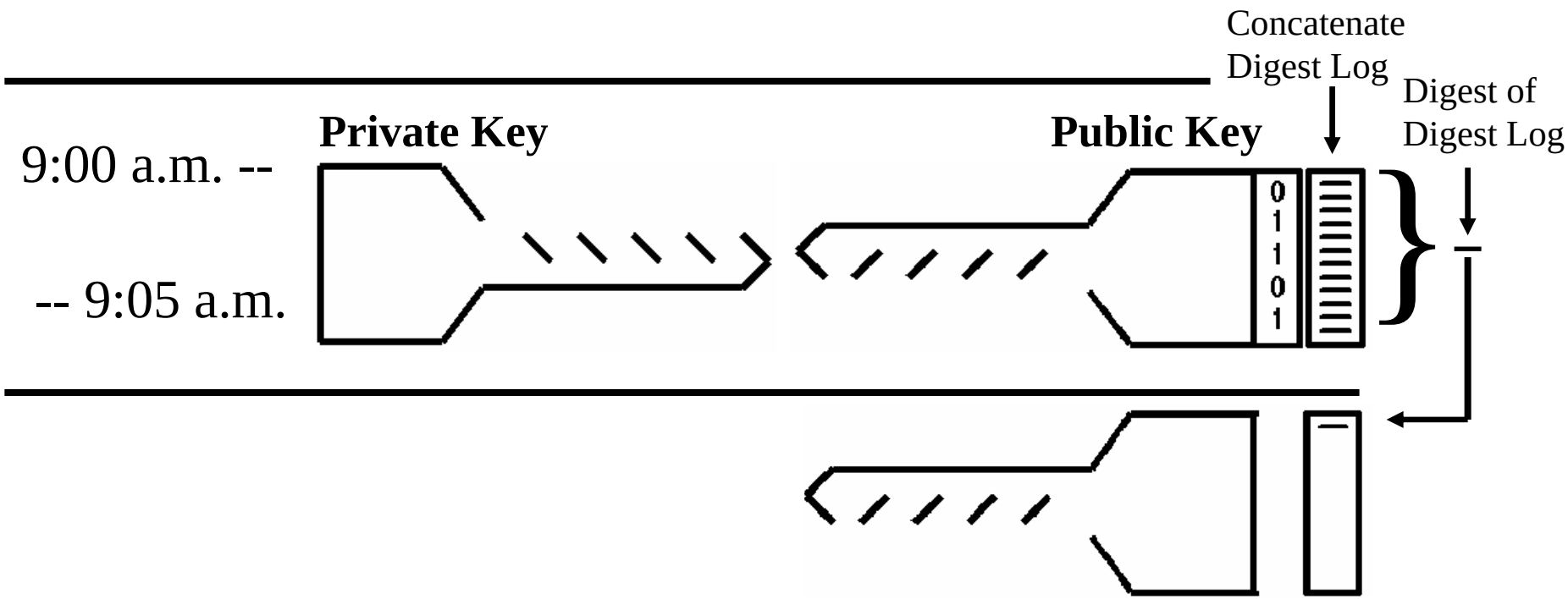
We create a concatenate digest log of all ProofMark requests



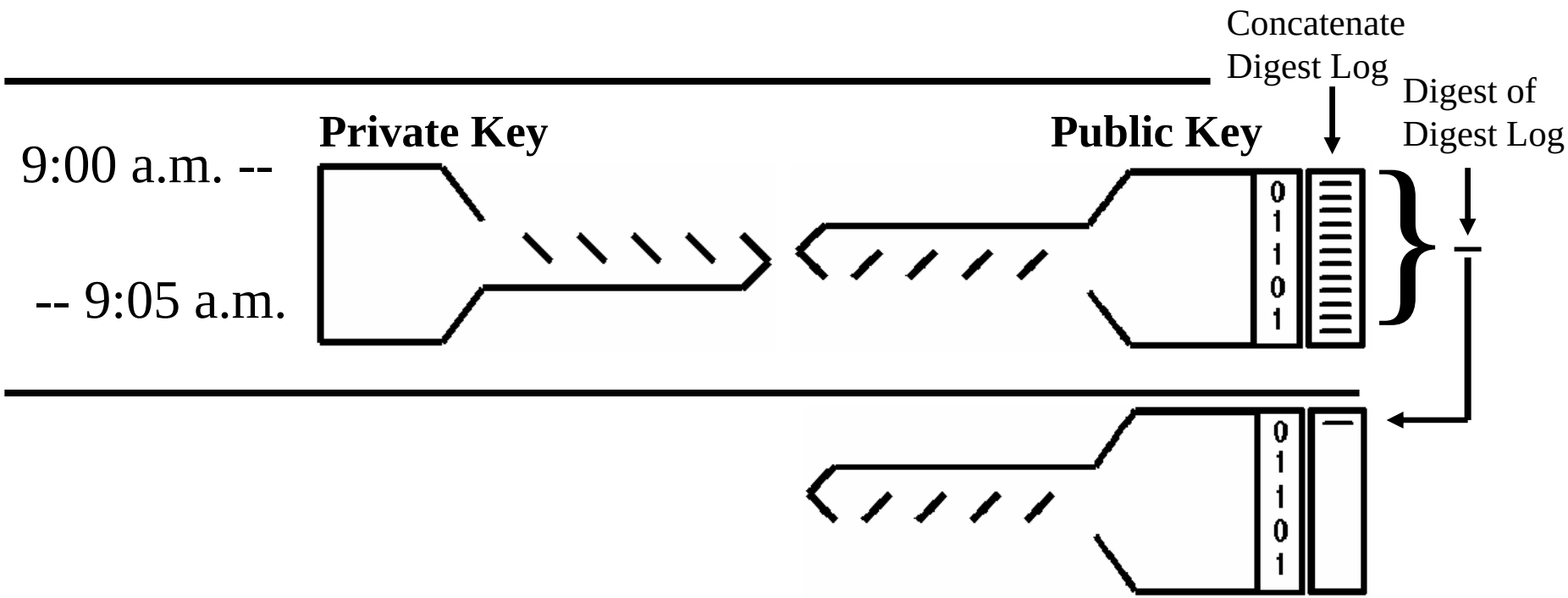
At the end of the interval, we create a digest from the digest log



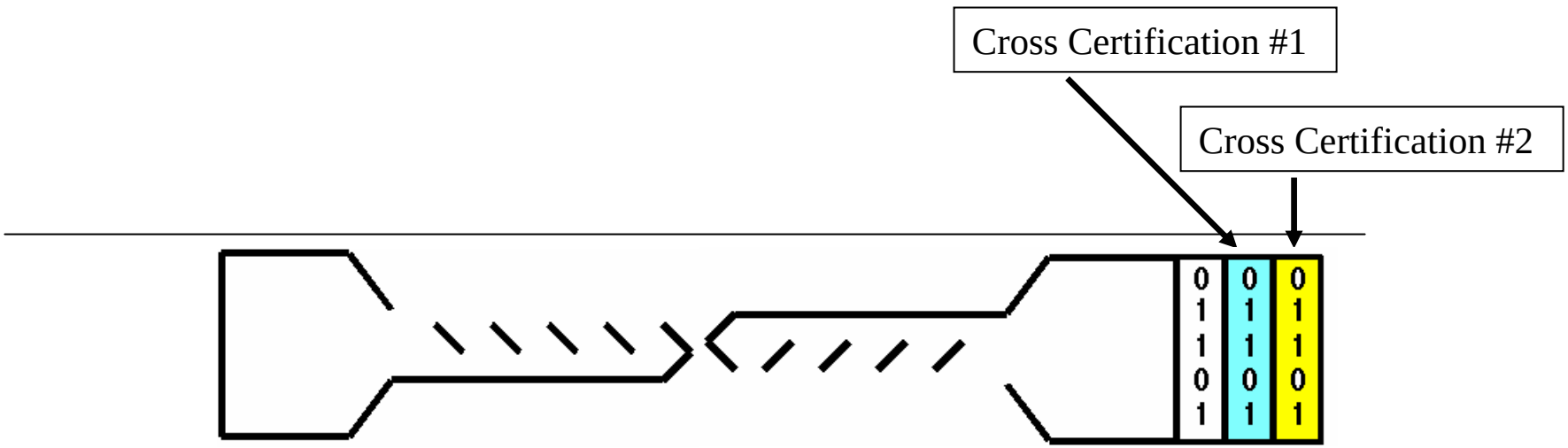
We then insert that digest into the new interval, prior to the signature by the prior private key



We then insert that digest into the new interval, prior to the signature by the prior private key

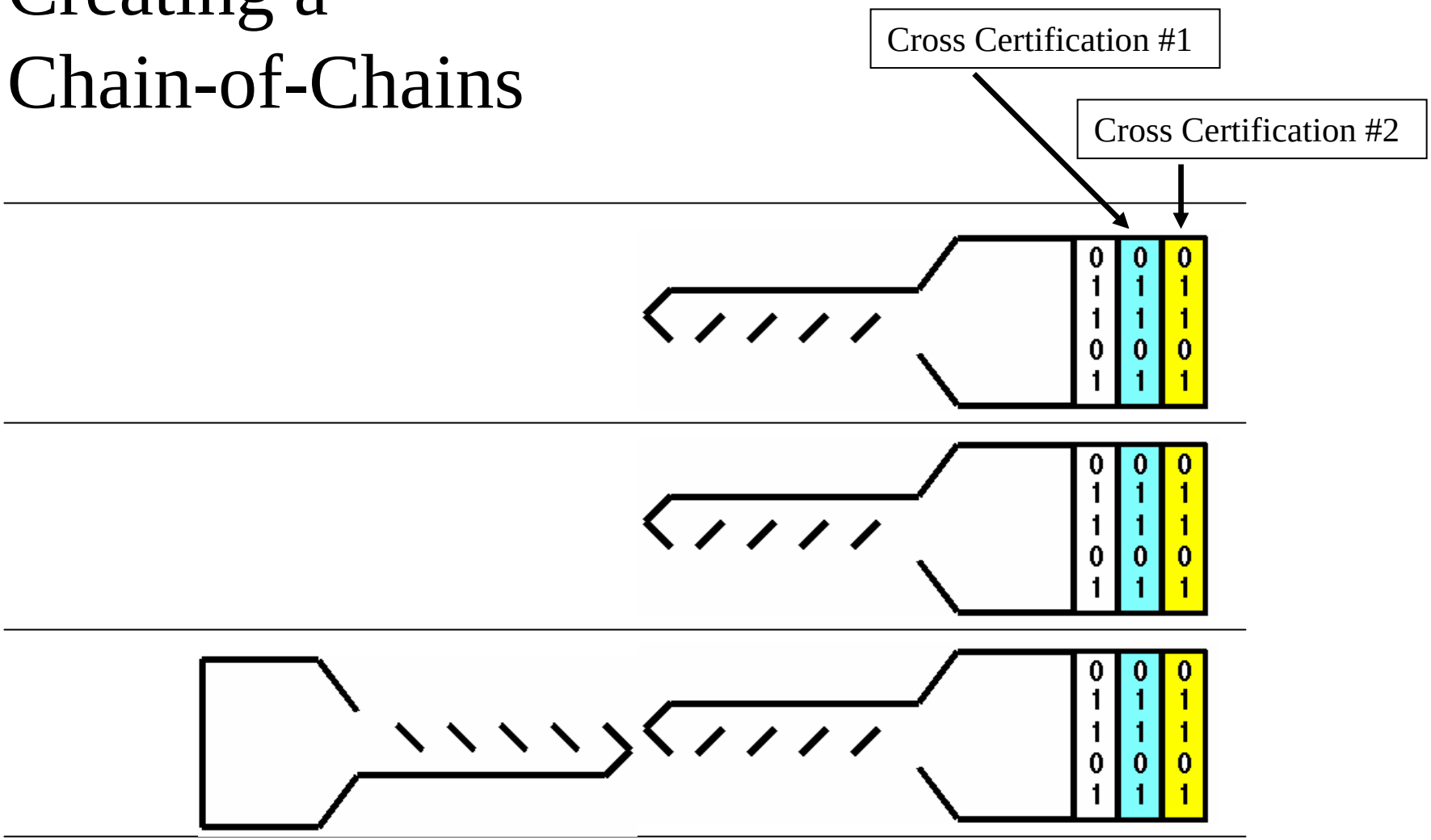


As a final protection against the compromise of a single chain, we cross certify with 2 other instances of the ProofMark System



proof space

Creating a Chain-of-Chains



proof space

The ProofMark System…

- Is a method of self-validating proof of time
- Creates Cryptographic Timestamps that never expire
- Is a fully distributed system
- Is immune from the compromise of secret keys
- Is independent of a Trusted Third Party
- Creates a network of validation & verification

A ProofMark Certificate Is A Suffix Of Data That Can Be Used To Prove The Integrity And Proof Of Time Existence For A Given Set Of Data...

Original Data	***ProofMark Certificate***
…010001100...	…10010...

proof space

A ProofMark Certificate Can Be Persisted...

Separately

Original Data	***ProofMark Certificate***
…010001100...	…10010...

Jointly

Original Data	***ProofMark Certificate***
…010001100...	…10010...

Or Within Your Data

Original Data	***ProofMark Certificate***
…010001100...	…10010...

ProofMark…

Tangible Proof In A Digital World!