Managing Enterprise Cybersecurity MIS 4596

Unit #12

Agenda

- Schedule Updates
- Identity and Authentication a historic problem
- Identity and Authentication for controlling access to IT Assets
- Identification
- Authentication
 - Something you know
 - Something you have
 - Something you are
- Multi-factor Authentication

Learning more about RSA

An online tool for checking your work:

https://www.cryptool.org/en/cto/rsa-step-by-step

Part 2. Calculating RSA keys

Note: To help you answer the following questions, view this "RSA Algorithm" video. Also, you can review the RSA wikipedia page example.

1. Complete encryption and decryption using the RSA algorithm, for the following data (show all work): p = 5, q = 11, e = 3, M = 9. Also:

Question: What is the ciphertext when performing RSA encryption with p=5, q=11, e=3, M=9?

Question: Show all work for encryption and decryption

2. You are Eve. In a public-key system using RSA, you intercept the ciphertext, C=10, sent to a user whose public key is e=5, n=35.

Question: What is the plaintext `M`?

<form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form>	ventuales step, by stop encopiliers or decopiliers with the REAL numbed. The ander uses the public key of the cyptom the recipient uses his associated private key to decopy.
<form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form>	ventuales step, by stop encryption or decryption with the REAL nucleid. The sender uses the public key of the cyption, the recipient uses the associated private key to decrypt.
<form><form><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><form><text><text><text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text></text></text></form></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></form></form>	ventuales step, by stop encryption or decryption with the REAL nucleid. The sender uses the public key of the cyption, the recipient uses the associated private key to decrypt.
<form><section-header><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form><form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></form></section-header></form>	syption; the recipient uses his associated private key to decrypt.
<form><form> Prime of the second s</form></form>	
<form><form> Name of the state of the state</form></form>	taatara
<form> A. a starding uperite fried Accesses the top preve 2 and 0. A. a starding prevention the top decision of the top decision of top decisio</form>	RSA is based on the fact that it is easy to calculate the product n of two large primes p and q. However, it is very
	nine only from the product n the two primes that yield the product. This decomposition is also called the factorizatio
model model <t< td=""><td>nt for RSA choose two primes p and q.</td></t<>	nt for RSA choose two primes p and q.
In the approxima to solve, the number process must be denoted approximation of a structure process must be approximation. In the approximation of a structure process must be approximated by a structure of a structure process must be approximated by a structure of a structure process must be approximated by a structure of a structure process must be approximated by a structure of a structure process must be approximated by a structure of a structure process must be approximated by	5
Auto screet floatands that y dight size used for scapes communications	7
P = P = Q $P = P = P = P = P = P = P = P = P = P =$	I to work, the two primes must be different. on we start with small primes. To make the factorization difficult, the primes must be much larger. Currently, values
<section-header> Public key</section-header>	ousand binary digits are used for secure communication.
The product is is able data module in the RSA method. The plattice hay constants of the module is and are exponent it. Product is is able data module in the RSA method. The plattice hay constants of the module is and are exponent it. $Product is is able data module in the RSA method. The plattice hay constants of the module is and are exponent it. Product is is able data module in the RSA method. The plattice hay constants of the module is and are exponent it. Product is is able data module in the RSA method. The plattice hay constants of the module is able data module in the RSA method. The RSA method is able of the RSA method is is a distinct in the RSA method is is able of the form of the RSA method is in the RSA method is interplate inte$	35 (6 BR)
The product is all or class thread the same for all platforganes. The new result is product is all platforganes. The second term is all platforganes. Second terms Second terms Bits uses the flat or electronic of the same for all platforganes . $(p_1 = p_1 = p_1 = (q_1 = p_1) = (q_1 = q_1) = (q_1 = q_2)$ The second term is all platforganes the second term ty. This is defined as $(p_1 = p_1 = p_1 = (q_1 = q_1) = (q_1 = q_2)$ The second term is all platforganes the flat or electronic term ty the is is defined as $(p_1 = p_1 = p_1 = (q_1 = q_2) = (q_1 = q_2)$ The definition for the same for all platforganes the flat or electronic disconding or flat of q_1 and q_2 are q_2 are differently determine q_1 (q_1 = q_2) = (q_1 = q_1) = (q_1 = q_2) The definition for the same for all and the platforganes the flat and q_2 are q_2 are differently determine q_1 (q_1 = q_2) = (q_1 = q_1) = (q_1 = q_2) The definition for the same for all and a d in the platforgane that is a same flat or q_1 (q_1 = q_1) = (q_1 = q_2) = (q_1 = q_1) = (q_1 = q_2) = (q_1 = q_2) = (q_2 = q_1) = (q_1 = q_2) = (q_1 = q_2) = (q_2 = q_1) = (q_1 = q_2) = (q_1 = q_2) = (q_2 = q_1) = (q_1 = q_2) = (q_2 = q_1) = (q_1 = q_2) = (q_2 = q_2) = (q_1 = q_2) = (q_2 = q_1) = (q_2 = q_2) = (q_1 = q_2) = (q_2 = q_2) = (q_2) = (q_	kov
remains the process of the sector stars to the participants is defined as $(1 + 1)^{-1} = 1$ for an ensure to the sector stars to the participant is defined as $(1 + 1)^{-1} = 1$ for an ensure star is a star base is defined as $(1 + 1)^{-1} = 1$. The series $(1 + 1)^{-1} = 1$ for a stars the stars of defined for the bacterian stars to define defined and stars the stars of the bacterian stars to define defined is defined as $(1 + 1)^{-1} = 1$. The series $(1 + 1)^{-1} = 1$ for a star base is the stars the stars of defined for the bacterian stars to define defined or function $(1 + 1)^{-1} = 1$. The series $(1 + 1)^{-1} = 1$ for a star base is the stars the stars of defined for the bacterian stars to define defined is the stars of the bacterian stars to define defined is the stars of the bacterian stars to define defined is the stars of the bacterian stars to define defined is the stars of defined is the stars of defined is the stars of the bacterian stars to define defined is the stars of defined	also called module in the RSA method. The public key consists of the module n and an exponent e.
The range of the sector $\mathbf{F}_{\mathbf{F}}$ is the fraction of the sector $\mathbf{F}_{\mathbf{F}}$ is the sector $\mathbf{F}_{\mathbf{F}}$	5
RAS uses the filter q includes of his calculate the second twy. This is defined as Second two is the filter q includes of his calculate the second twy. This is defined as $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of his calculate the second twy. This is defined as $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of the target common divisor must be (1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of p(1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of p(1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of p(1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of p(1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of p(1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter q includes of p(1). $q(r) = f(p + 1) + (q - 1)$ (0) RAS uses the filter $q(r) + q(r)$ $q(r) = f(q + 1) + (q - 1)$ (0) (0) RAS uses the filter $q(r) + q(r)$ $q(r) = f(q + 1) + (q - 1)$ (0) (0) RAS uses the filter $q(r) + q(r) + q(r)$ $q(r) = f(q + 1) + (q - 1) + (q + 1$	be pre-selected and the same for all participants.
Ref Lagor 9 Location 4 to conclude the sector lag, this is addited as Ref Australia C $(q_1 = (q_2 - 1) + (q_1 - 1)$ $(q_2 - 1) + (q_1 - 1)$ Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 9 binction is copiene to e (the largest common divisor must be 1). Here 8 is upportant for RSA half the value of the 1 binction divisor must be 1. C of copien values of 0, e and e a weight with regard to a result with the result of 0. The decommon divisor (the 1 - 1) of the 0 constant for the result with regard to a result with regard to a result with regard to a result with the result of 0. The decommon divisor (the 1 - 1) of the 0 constant for the result with regard to a result with rega	less.
q(r) = (p - 1) + (q - 1) $d0$ $q(r) = (p - 1) + (q - 1)$ $q(r) = (p - 1) + (q - 1)$ Here its used hild p and q and different. Otherwise, the q functions vacuum	Key life q function of n to calculate the secret key. This is defined as
Here is used that pand part and different. Otherwise, the is placeting the placeting and the placeting and the placeting the placeting to be p	
The properties for scales the solution is a specified to a result of the algobia common double fruction (). $ \begin{aligned} \mathbf{p}(\mathbf{r},\mathbf{r},\mathbf{r}) & \mathbf{r} $	
$e^{e(t_{i}, e^{e(t_{i})}}$ 1 $e^{e(t_{i}, e^{e(t_{i})}}$ To demonstre the value of $\phi_{i}(t_{i})$ is the source $\phi_{i}(t_{$	iat ρ and φ are different. Otherwise, the φ function would calculate differently. r RSA that the value of the φ function is coprime to e (the largest common divisor must be 1).
To determine the value of φ_1 if it is not anough to know 1 only with the knowledge of φ and φ we can efficiently determine φ_1 : The second key also constants of a and a d' with the property that $e \times d$ is a multiple of φ_1 plus one. Expresses to thoradas, the fibriary grant expression of φ_1 and $e \times \varphi_2$ plus a constant of a low of the exist as a multiple of φ_1 plus one of f there is an integer a transmission of φ_2 and φ_2 with regards that exceeds key that $\varphi_1 = \varphi_2$. The document with the problem when equality with regards to a resolute (keys, it is $x \times y$ (mod 2) if and only if here is an integer a transmission of φ_1 and φ_2 with regards to a resolute (keys, it is $x \times y$ (mod 2) if and only if here is an integer a transmission of φ_1 and φ_2 with regards to a resolute (keys, it is $x \times y$ (mod 2) if and only if here is an integer a transmission of φ_1 and φ_2 with regards to a resolute (keys, it is $x \times y$ (mod 2) if and only if here is an integer a transmission of φ_1 and φ_2 with regards to a resolute (keys, it is a resolute (keys), it	1
The sector key also consists of m and a d m for graphing mate is d in a mininge of opin (put sets). The sector key also consists of mate is a dim for graphing mate is d in a mininge of opin (put sets). The sector key also consists of the consists of the consist and the graphing mate is d in a mininge of opin (put sets). The sector key also consists of the consists of the consists of the restaute cases. It is $x = y$ (mod 2) if and only if here is an integer a mininger a mininger a mininger a mininger of the mate case is the set of the consists of the material of the material of the consists of t	value of $\varphi(n)$, it is not enough to know n. Only with the knowledge of p and p we can efficiently determine $\varphi(n)$.
$e_1 < 1$ (mod $q_1(t)$) But provide the first set of the provide q_1 (the set of the provide q_2 (the se	value of $\psi(n)$, it is not enough to know <i>n</i> . Only with the knowledge of p and ψ we can enciency determine $\psi(n)$. Iso consists of <i>n</i> and a <i>d</i> with the property that <i>e</i> × <i>d</i> is a multiple of $\psi(n)$ plus one.
The decision of the depresentation means regarding with regarding and the set restriction described above) - for example with the extended Euclidean above - for example above - for example with the extended Euclidean above - for example	mulas, the following must apply:
Provide chosen values of j_1 q_2 and q_1 we get d as: a' 2^{2} The can always be adtermined (if e was chosen with the instruction discorded above)—for example with the instruction Euclidisen agostim. Encryption and decryption Instrudy, the method works only with numbers too locity, which are between 0 and is Encrypting a missage in (number) with the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. These allows and groups and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging a missage in (number) with the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. These allows and groups and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated by the policie key, and then policie key. $m^{2} = m^{2} \pmod{3}$. The other does does and the method we with the policie key. $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated by the policie key, and then policie key. $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated by the policie key. $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated by the policie key. $m^{2} = m^{2} \pmod{3}$. Becogging and the policie key (is, e) is calculated by the pol	(n)) mod expression means equality with regard to a residual class. It is x = y (mod z) if and only if there is an integer a
a^{-1} 2^{-1} The dra always be determined (if e was chosen with the restriction described above)—for example with the extended Euclidean algorithm. The dra always are determined (if e was chosen with the restriction described above)—for example with the extended Euclidean algorithm. Encryption and decryption Encryption and decryption Internally, its method works only with numbers (to led), which are between 0 and 0. Encryption ansauge (internally, its method works only with numbers (to led), which are between 0 and 0. Encrypting a message (internally). The dra always device (internally) are analogously with any field of a calculated of $a^{-1} \sim a^{-1}$ (mod n). The dra always device analogously with any field of a calculated of $a^{-1} \sim a^{-1}$ (mod n). This de all draves chosen appropriately, if is (internally). $a^{-1} = a^{-1}$ (mod n). The dra draves of chosen tradepropriately, if is (internally). As and draves chosen appropriately, if is (internally). $a^{-1} = a^{-1}$ (mod r). $a^{-1} = $	1
The draw easys be determined (if e was chosen with the instruction detortion above)—for example with the extended Euclidean agortim. The draw laws gradient instruments to be too, which are between 0 and n Encrypting an easage (in runner) with the public key (in, in) are between 0 and n Encrypting an easage (in runner), with the public key (in, in) are between 0 and n Encrypting and easage (in runner), with the public key (in, in) are between 0 and n Encrypting and easage (in runner), with the public key (in, in) are between 0 and n Encrypting and in the public key (in, in) are between 0 and n Encrypting and in the public key (in, in) are determined in "= m ² (mod n), Bids how experiments $m^2 = m^2 (mod n),$ $m^2 = m^2 (mod n$	alues of p, q, and e, we get d as: 5
Encryption and decryption Encryption Interval, the nettor solar only with numbers too bads, which are between 0 and n Encryption Encryption anessage (interval), with numbers too bads, which are between 0 and n Encryption Encryptig an ensage (interval), with numbers too bads, which are between 0 and n Encryptig and massage (interval), the number of the public key (n, e) is calculated: $n^+ = n^+$ (mod n), $n^+ = n^+$ (mod n), $n^+ = n^+$ (mod n), RDA one expection of the public key (n, e) and the metallised by the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key (n, e) is an end of the public key. If the public key (n, e) is an end of the public key (n, e) is an end of the public key. $n^+ = n^+$ (mod n),	5 is be determined (if e was chosen with the restriction described above)—for example with the extended Euclidean
Internativ, this method works only with numbers (no body, shich are between 0 and n Encrypting a missage (number) with the public key (n, n) a carculated: Encrypting a missage (number) with the public key (n, n) a carculated: Encrypting a missage (number) with the public key (n, n) a carculated: The ner = a^n (nod n). $a^n + a^n$ (nod n). $a^n + a^n$ (nod n). The ner $m^n = a^n$ (nod n). $m^n = a^n + a^n$ (nod n). The Ner $m^n = a^{n-1}$ (nod n). $m^n = a^{n-1}$ (nod n). The Access equation of node node node node node node node node	
Internally, this method scores only with numbers (to they, include extension 1 and 1. Internally, this method scores only with numbers (to they, include extension 2 and 1. Encypting a maximum score (include extension) Encypting a maximum score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include (include extension) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ (include extension) Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$ Internally, this method score (include extension) Internally, this method score (include extension) $m^* = m^0$	tion and decryption
$m^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ Decipiting with the plantite key (n, d) is done assidgously with $m^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ The is $m^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ This is RA now explosible the plantite key (n, d) is done assidgously with $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ This is $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = a^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ $m^2 (man n)$ $n^2 = m^2 (mod n)$ $m^2 = m^2 (mod n)$ $n^2 = m^2 (mod n)$ m	ethod works only with numbers (no text), which are between 0 and n.
Decipiting with the private key (iii) is done analogously with $d = 1 + a d^2 \log d$ $m^2 + a d^2 (\log d)$ $m^2 + a d^2 \log d$ The is $m^2 + a d^2 + (\log d)$ $m^2 + a d^2 + (\log d)$ $d = b (\log d) (m)$ $d = b (\log$	ssage m (number) with the public key (n, e) is calculated.
$\begin{array}{c} m^2 = m^2 (\operatorname{mod} m), & m^2 = m^{2-2} (mo$) the private key (n, d) is done analogously with
$m^{+} = m^{++} f(mod n) \qquad $	
In this how explosition the projecting that $r = 0$ (mod 2) and $r = 0$ (mod 2) or $r = $	
x* = x*(nod in) x* = x*(nod in) x x* = x*(nod in) x* = x*(nod in) x* = x*(nod in) x = x = 0 frood giv(i) x x = 0 frood	I n). Is the property that
a = b (mod qVr) A e and d wave chosen appropriately, it is m ⁺ e.n. The ender does not matter You could also first rate a message with the prate key, and then power up the result with the public key — that is with you with TGA supportances. The ender use with TGA supportences.	
As e and zwee closen appropriately, is a m ⁺ e.m. The ender does not matter You could also that raise a message with the prate key, and then power up the result with the public key — The ender use with TSAs spatients. The ender use with TSAs spatients. The ender use with TSAs spatients.	
m ⁺⁺ = m. The order does not matter You could also first rate a message with the private key, and then power up the result with the public key m ⁺⁺ = m. —Insis what you use with RSA signatures. The order does	chosen appropriately, il is
-this is what you use with RSA signatures. The order does	
	not matter. You could also first raise a message with the private key, and then power up the result with the public ke u use with RSA signatures.
Messages	
In the following has beet howes, you can see how the encryption and decording works for concrete input (numbers).	-
plaintext 9	wo text boxes, you can see how the encryption and decryption works for concrete input (numbers).
plantext	5
cipheriox 14	

CRYPTOOL-ONLINE

C CRYPTOOL-ONLINE

MIS 4596

Identity and Authentication

"...is about the continuity of relationships, knowing who to trust and who not to trust, making sense of a complex world"

(Schneier, Secrets and Lies, p. 68-69)

• Are ancient problems, a Bible example, from approximately 1100 BC talks about the Gileadites who captured the water crossings of the Jordan river leading to Ephraim...,

Damascus Basha M AN Ashtaroth S S EH ank River **Ramoth Gilead** Beth Arbel Sea of Galilee Gadara DECAPOLIS **Beth Yerah** Lo Debar 1sh Je Jordan River Jabesh iilea Jabbok River Pehel Beth Shan J. Umm ed-Daraj e Harod Valley 9 Rif

~

Zaphon

0

レ

9

Penuel/Peniel

Mahanaim

Succoth

Rabbah (of the Ammonites)

Gedor

9

G A D



5 And the Gileadites took the passages of Jordan before the Ephraimites: and it was so, that when those Ephraimites which were escaped said, Let me go over; that the men of Gilead said unto him, Art thou an Ephraimite? If he said, Nay;

6 Then said they unto him, Say now Shibboleth: and he said Sibboleth: for he could not frame to pronounce it right. Then they took him, and slew him at the passages of Jordan: and there fell at that time of the Ephraimites forty and two thousand.

Judges 12:5-6

shibboleth

More recently, the word "Shibboleth" has been incorporated into the English language to mean something that distinguishes or identifies someone:

 a peculiarity of pronunciation, behavior, mode of dress, etc., that distinguishes a particular class or set of persons

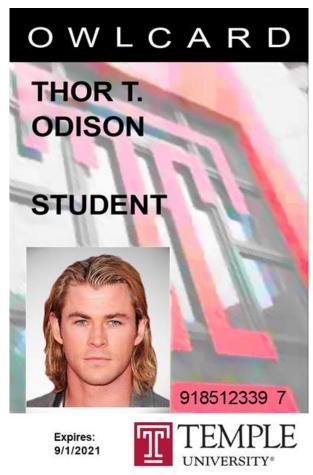
Talking like a stereotypical New Yorker



Question:

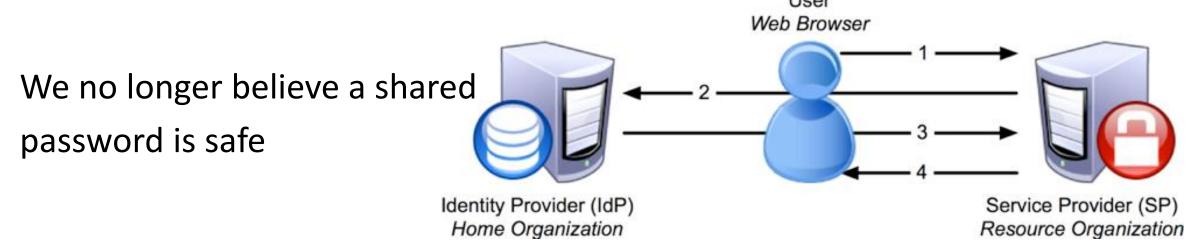
When you enter Speakman or Alter Hall and show/swipe your Temple ID, what is happening?

- Identification ?
- Authentication ?
- Authorization ?



shibboleth

In today's information technology a shibboleth is a single shared community-wide password that enables members of that community to access an online resource without revealing their individual identities



Shibboleth.

Identity Provider

Controlling Access to IT Assets

- A central theme of information system security
- Many different security controls work together to provide access control
 - Identity, Authentication, Authorization, Auditing...
- IT Asset includes:
 - Information
 - Systems
 - Devices
 - Facilities
 - Personnel



Identity Management

Identification and Authentication are distinct functions

Identification: Who you say you are

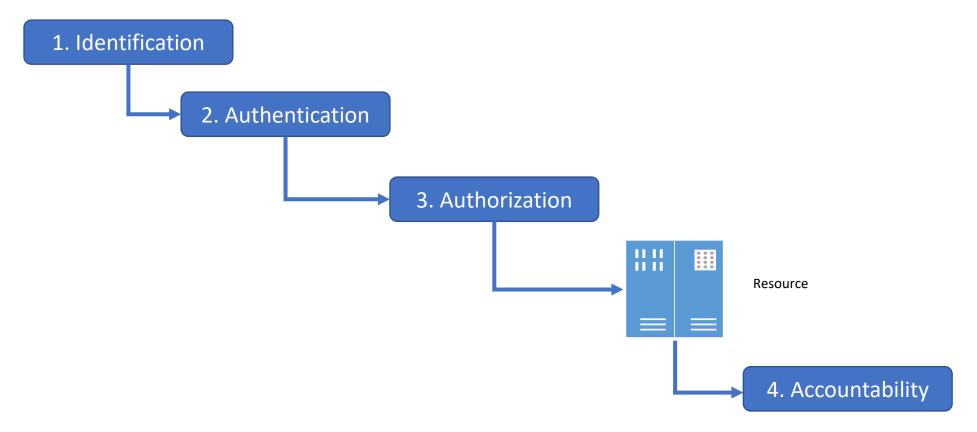
Authentication: Confirmation that you are who you say you are

Identity and Authentication

First line of defense in battling unauthorized access to network resources and systems

 Broad term covering several types of mechanisms that control access to features of networks, computers and information stored and flowing within them Identification, Authentication, Authorization, and Accountability ("AAA")

To access an information system resource, a user must pass through the following logical steps:



Authorization: Access to information...

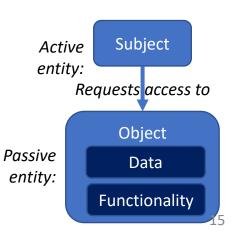
Access is the ability to create a flow of information between user and system

The flow of information between a <u>subject</u> and an <u>object</u>

- Subject
 - Always the active entity requesting access to an object or data within the object
 - Can be users, programs, processes, services, computers...
 - When authorized, subjects can modify objects
- Object
 - Always the passive object providing information to active subjects
 - Can be data files, databases, computers, programs, processes, services, storage media...

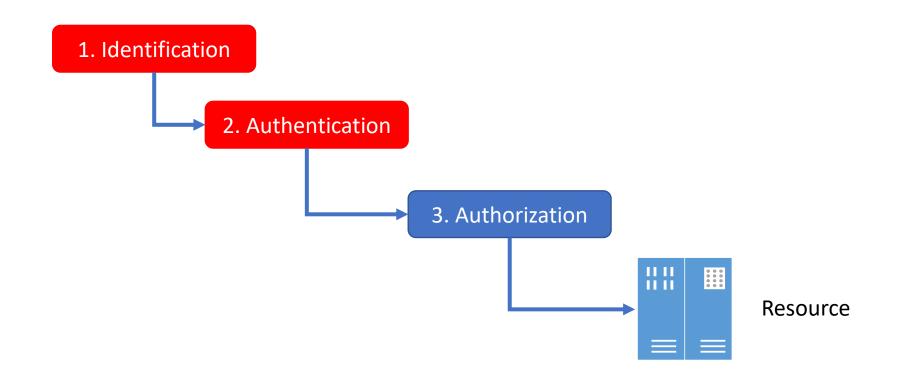
E.g. "A user (subject) accesses an object (data file)"

Note: Roles of subject and object can switch during interactions – e.g. a computer program can be both a data requester and a data provider, switching back and forth



To access a network's resource, a user must:

Prove their identity (i.e. has the necessary credentials)



Identification and Authentication

Usually involves a two-step process:

1. Identification: Entering public information

- Method by which a subject (user, program or process) claims to have a specific identity
 - Username, employee number, account number, or email address

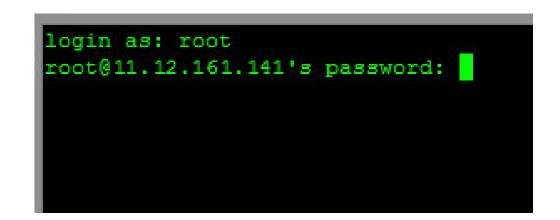
2. Authentication: Entering private information

- Individual's identify must be verified during authentication process
- Method by which subject proves it is who it says it is
 - Static password, smart token, one-time password, or PIN

Identification

Method of establishing the subject's identity

- Subject can be a human user, program or process
- Identity A set of attributes that <u>uniquely</u> describe a person within a given context
- Typically a user name, email address or other public information





Identification



Entering public information

- Method by which a subject (user, program or process) supplies identifying information to claim they have a specific identity
 - Username, employee number, account number, or email address

Creating secure identities involves 3 key aspects:

- **1. Uniqueness** every user, program or process must be identified with an identifier (i.e. unique ID) that is specific to the individual for accountability
- **2. Non-descriptive** Identifier should not indicate the purpose of the account nor the user's position nor tasks done with the account
- **3. Issuance** provided by an authority as a formal/official means of proving identity

Authentication

The process of establishing confidence in the identity of users or information systems

Method of proving identity is something a person:

- 1. Knows a secret password
- 2. Has a public key certificate, Computer Access Card, ...
- 3. Is or does biometrics



Authentication – Classic 3 factor paradigm

... for authentication systems

Subject provides information to prove it is who it says it is and authentication system verifies the identification information

- **1. Something the subject knows** ("authentication by knowledge") Type 1 factor
 - Examples: password, PIN, combination to a lock...
 - Usually least expensive method to implement
 - Vulnerability: Someone else may acquire this knowledge and gain unauthorized access to a resource

2. Something the subject has ("authentication by ownership") – Type 2 factor

- Examples: Key, swipe card, access card, badge...
- Common for accessing facilities, sensitive areas, and authenticate holder
- Vulnerability: Can be lost or stolen and result in unauthorized access
- **3. Something the subject is** ("authentication by characteristic") Type 3 factor
 - Examples: Fingerprint, palm scan, retina scan...
 - Based on biometrics a way to identify the subject by a unique physical attribute
 - Vulnerability: Can be expensive, cumbersome/troubling to users and associated with false acceptance or rejection

Authentication – <u>Something you know</u>

Use of secret words to authenticate humans dates at least as far back as the military of ancient Rome (Polybius, 118 BC), which developed a careful procedure for using daily "watchwords" to prevent infiltration

Also appears in the folk tale of Ali Baba and the forty thieves (translated into English in 1785) who used the phrase "open sesame" to access a magic cave



Authentication – something you know

Passwords

- A secret shared between user authentication system
- User name + password most common identification, authentication scheme
 - A weak security mechanism requiring implementation of strong password protections

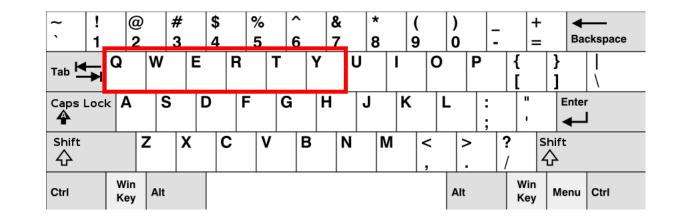


Authentication - Passwords

How many unique characters can be produced by the standard QWERTY keyboard?

Standard US Qwerty keyboards have 101, 104 or 107 keys which can produce 96 unique characters

- 26 lower case letters
- 26 upper case letters
- 10 numbers
- 32 visible symbols
- 2 Windows and Menu keys



"The name comes from the order of the first six keys on the top left letter row of the keyboard (Q W E R T Y). The QWERTY design is based on a layout created for the Sholes and Glidden typewriter and sold to E. Remington and Sons in 1873. It became popular with the success of the Remington No. 2 of 1878, and remains in widespread use."

Wikipedia

Authentication – Classic 3 factor paradigm

... for authentication systems

Subject provides information to prove it is who it says it is and authentication system verifies the identification information

- **1. Something the subject knows** ("authentication by knowledge") Type 1 factor
 - Examples: password, PIN, combination to a lock...
 - Usually least expensive method to implement
 - Vulnerability: Someone else may acquire this knowledge and gain unauthorized access to a resource

2. Something the subject has ("authentication by ownership") – Type 2 factor

- Examples: Key, swipe card, access card, badge...
- Common for accessing facilities, sensitive areas, and authenticate holder
- Vulnerability: Can be lost or stolen and result in unauthorized access
- **3. Something the subject is** ("authentication by characteristic") Type 3 factor
 - Examples: Fingerprint, palm scan, retina scan...
 - Based on biometrics a way to identify the subject by a unique physical attribute
 - Vulnerability: Can be expensive, cumbersome/troubling to users and associated with false acceptance or rejection

Authentication - Passwords

How to create a password that is hard to crack:

- The longer the password, the harder it is to crack
- Always use a combination of characters, numbers and special characters
- Variety in passwords on different apps and systems...

https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

 1 character password: 	96 tries to crack
 2 characters: 96 *96 = 	9,216
 3 characters: 96 * 96 * 96 = 	884,736
 4 characters: 96⁴ = 	84,934,656
•	
 8 characters: 96⁸ = 	7,213,895,789,838,336
•	
. –	

• 15 characters: 96¹⁵ = 542,086,379,860,909,058,354,552,242,176

LAST XJJW TONIGHT

Authentication: Passphrase

This is a relatively complex password: cCs,.ebj7L}c But it is difficult to remember

Passphrase

- Is a sequence of characters that is longer than a password
- Takes the place of a password
- Can be more secure than a password because it is more complex

This passphrase is easier to remember:

I like to eat chocolate chip cookies.

Use of random words in passphrase is better: Correct horse battery staple



"The reuse of passwords is the #1 cause of harm on the internet"

https://www.cnet.com/news/facebook-chief-securityofficer-alex-stamos-web-summit-lisbon-hackers/

Users reuse passwords



12%-43%* reuse rate

*"Data breaches, phishing, or malware?"

According to a study of 29 million people, 38% reused their passwords

https://arxiv.org/pdf/1706.01939.pdf

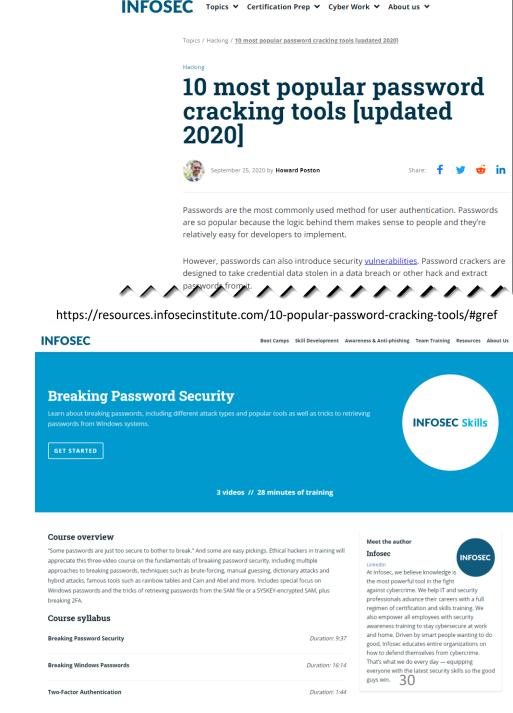
Research at Google

https://static.googleusercontent.com/media/research.google.com/ en//pubs/archive/46437.pdf²⁹²⁹

Techniques to attack passwords

- Guessing
- Social engineering
- Dictionary attacks
- Electronic monitoring
- Access the password file
- Brute force attacks
- Rainbow tables





MIS 4596

Authentication: Passwords with Password Managers

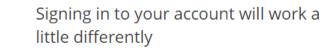
Keeping all of your passwords in a password manager is a good idea

- https://en.wikipedia.org/wiki/1Password
- <u>https://en.wikipedia.org/wiki/LastPass</u>
- <u>https://fossbytes.com/best-free-password-manager-software/</u>
- <u>https://www.techradar.com/best/password-manager</u>

Authentication - something you have

e.g.

- Your phone
- ID Card
- Synchronous token
 - Time Based
 - Counter Synchronization





Whenever you sign in to Google, you'll enter your password as usual.

You'll be asked for something else

Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.



Identification Card





User logs into an account

using their primary password

2

123456



An authentication code (OTP) is

sent to the user's mobile phone

•



3

User enters the OTP as the secondary password and is granted access to their online account



...something you have: Cell phone

The number one thing most people can do to protect themselves online is to enable any type of two-factor authentication for their important accounts



2-factor authentication requires you to have 2 things to get into your account, often it consists of:

- 1. Something you know (your password)
- 2. Something you have
 - 1. Your mobile device with security code

SMS stands for Short Message Service, the most widely used type of text messaging

- When you enable SMS-based 2-factor authentication, the service will send your mobile phone number a text message containing a one-time code whenever you sign in from a new device
- If someone has your username and password for the related account, they cannot sign into your account without access to your text messages

Google

2-Step Verification

This extra step shows it's really you trying to sign in



2-Step Verification

A text message with a 6-digit verification code was just sent to (\cdots) $\cdots \cdots$

G-

Don't ask again on this computer

Something you have: Cell phone

SMS-based 2-factor authentication is better than nothing, but still not ideal because someone could steal your phone number or intercept your text messages

For example,

An attacker could impersonate you and move your phone number to a new phone

- In a "Port-out scam" a criminal pretends to be you and moves your current phone number to another cellular carrier
- In "SIM hijacking", an attacker moves your phone number from your current SIM card to the attacker's SIM card

This is a big problem!

• Many online accounts, including bank accounts, use your phone number as a two-factor authentication method. They won't let you sign in without sending a code to your phone first.

But, after the porting scam or SIM hijacking has taken place, the attacker will receive that security code on their phone. They can use it to gain access to your financial accounts and other sensitive services.

Something you have: Cell phone

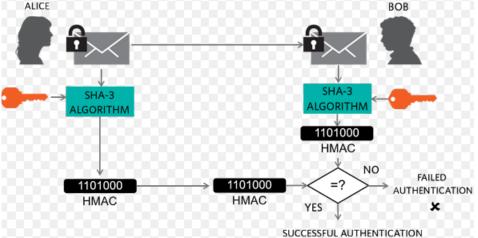
- SMS-based 2-factor authentication is not ideal because someone could steal your phone number or intercept your text messages
 - It's one of the weaker things that you can have to authenticate, because your phone number is actually "something you lease" from the phone company, you don't actually own or control it
- For example, in the most likely attack
 - An attacker could impersonate you and move your phone number to a new phone in a <u>phone number porting scam</u>
- Alternatively, an attacker could intercept SMS messages intended for you
 - For example, they could spoof a cell tower near you, or a government could use its access to the cellular network to forward and capture your messages

Something you have: Cell phone with one-time codes

• Hash (HMAC)-based one-time password (HOTP),

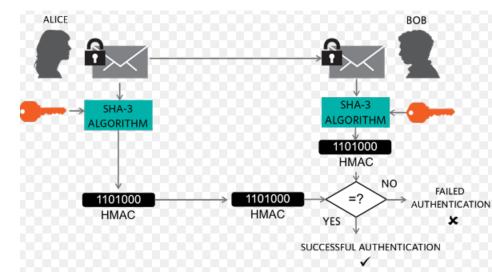
https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm

- HMAC = Hash Message Authentication Code
- 1. Message is concatenated with a symmetric key (not encrypted,
- 2. The combination is hashed resulting in a HMAC
- 3. The HMAC is appended to the message and sent to the receiver
- 4. The receiver concatenates the message with the symmetric key
- 5. The receiver hashes the combination and compares it to the HMAC received with the message, if the HMACs match the message is authenticated
- Note: Authenticity and Integrity are achieved, but confidentiality is not



Something you have: Cell phone with one-time codes

- Hash (HMAC)-based one-time password (HOTP), <u>https://en.wikipedia.org/wiki/HMAC-based_One-</u> <u>time_Password_algorithm</u>
- Time-based one-time password (TOTP), <u>https://en.wikipedia.org/wiki/Time-based_One-</u> <u>time_Password_algorithm</u>



 Drawback is that these can be phished, intercepted, and man-in-themiddle attacked

Something you have: Universal Second Factor (U2F) security keys

- U2F security keys turn web authentication on its head
 - Instead of the user having to authenticate to the website, U2F requires websites to authenticate to the U2F token
- It takes people out of the authentication equation, making phishing impossible
- <u>Google eliminates phishing of its employees</u> requiring all employees to use U2F



https://en.wikipedia.org/wiki/Universal_2nd_Factor

Sites that let you use U2F: <u>https://www.dongleauth.info</u>

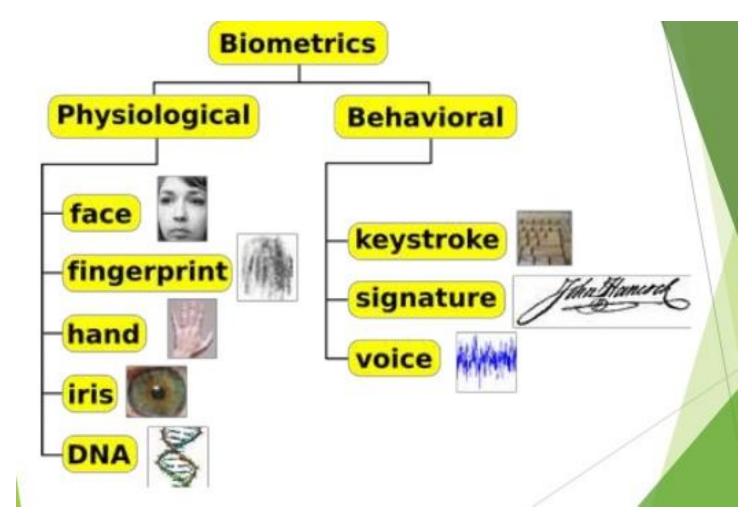
Authentication – <u>something you are</u> or do ("Biometrics")

- Verifies an identity by analyzing a unique person attribute or behavior
- Most expensive way to prove identity, also has difficulties with user acceptance
- Many different types of biometric systems



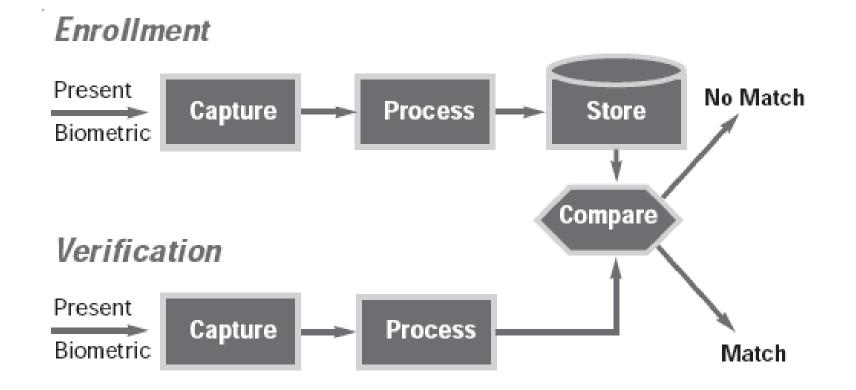
Authentication

Most common biometric systems:



Authentication – Biometric Systems

During identity verification (i.e. authentication) the biometric system scans personal's physiological attribute or behavioral trait and compares the captured data to a record created in an earlier enrollment process



Scanning fingerprint from display



Authentication: Multi-factor

Multi-factor authentication refers to use of >1 factor: Something the subject knows ("authentication by knowledge") + Something the subject has ("authentication by ownership") + Something the subject is ("authentication by characteristic")

Authentication system strength determined by the number of factors incorporated into the systems

- Implementations that use 2 factors are considered stronger than those that only use 1 factor
- Systems that incorporate all 3 factors are stronger than systems that incorporate 2 factors

Example: An ATM machine requires both something you have (the ATM card) and something you know (the PIN)

- Both the card and pin on their own are weak
- Together they are strong!

Authentication: Multi-factor

https://tuportal6.temple.edu/es/web/its/multi-factor-authentication

MULTI-FACTOR AUTHENTICATION

Overview

To better protect your personal information, Temple uses an extra level of security on selected websites called **Multi-Factor Authentication (MFA)**. It's called Multi-Factor Authentication because in order to access these sites, you will need:

your AccessNet username and password
 one or more designated phones to further verify your identity

Once you set up MFA, the next time you log in to a Temple website, such as TUportal or Canvas, you will first enter your AccessNet username and password. You will then be prompted to choose a verification method for the phone you registered for Multi-Factor Authentication.

Two Step Verification

Confirm Your Identity

This application requires a second verification step. Our system can call or text you, or if you have the Duo Mobile app installed, send you a passcode or approval screen

Getting an Access Denied / System Administrator message



Get Started: One-Time Setup

In TUportal, you can designate all your phones or particular ones for Multi-Factor Authentication, including mobile phone (smartphone or basic cell phone), landline, and TTY devices. To begin, click below and follow the instructions:

Designate a Phone for Multi-Factor Authentication...

Using Multi-Factor Authentication

When accesing a Temple website that uses Multi-Factor Authentication, such as TUportal and Canvas, you will be prompted to select a designated phone number and then a verification method. For instructions on logging in see the verification methods below:

Send Me a Push (Smartphone - Highly Recommended)...

Verification Option Description

nd Measure and an an



 \sim



✓ RSA Asymmetric Encryption Lab

✓ Identity and Authentication – a historic problem

✓ Identity and Authentication for controlling access to IT Assets

 $\checkmark \mathsf{Identification}$

✓ Authentication

✓ Something you know

✓ Something you have

✓ Something you are

✓ Multi-factor Authentication