1/6/2017 2ο επαναληπτικό μάθημα

Πρωτόκολλα Δημόσιου Κλειδιού

	RSA	El Gamal	Merkle-Hellman	Rabin
Δημιουργία κλειδιού	$n=p\bullet q$ e : $\gcd(e, \varphi(n))=1$ d : $e\bullet d\equiv 1(\mathrm{mod}\varphi(n))$	p, generator g $g^a \mathrm{mod} p$	Super-increasing a w,n : $\gcd(w,n)=1$ $b_i=a_i\bullet w(\mathrm{mod}n)$	
Κρυπτογράφηση	$C=M^e \mathrm{mod} n$	$\gamma=g^k \mathrm{mod} p$ $\delta=M\bullet g^{ak} \mathrm{mod} p$	Σπάω το Μ σε block $c_i=\Sigma(b_i m_i)$ m_i τα bit μηνύματος	
Αποκρυπτογράφηση	$M=C^d \mathrm{mod} n$	$M=\gamma^{p-1-a}\bullet\delta$	$c_i \rightarrow c_i \bullet w^{-1} \mathrm{mod} n$	

Γνωστά δημόσια, ιδιωτικά

Γενικά στα θέματα τα νούμερα θα είναι μικρά, αλλά θα πρέπει να εφαρμόσουμε τη ζητούμενη μέθοδο και να μην κάνουμε εξαντλητική αναζήτηση.

Θέμα (4 μονάδες)

Έστω ότι έχουμε RSA: C=5, (n,e)=(119,35) και δίνεται ότι 119=7•17. Ποιο είναι το μήνυμα Μ;

Απάντηση: Ζητείται το αρχικό μήνυμα και ζητείται το κρυπτογραφημένο μήνυμα και το δημόσιο κλειδί. Άρα θα πρέπει να κάνουμε αποκρυπτογράφηση, $M=C^d \mathrm{mod} n$. Βλέπουμε ότι πρέπει να υπολογίσουμε το d:

Από την αρχικοποίηση, έχουμε ότι $e\bullet d\equiv 1(\mathrm{mod}\varphi(n)) \rightarrow 35\bullet d\equiv 1(\mathrm{mod}96)$ και πρέπει $\gcd(35,96)=1$ για να έχει λύση η εξίσωση. Εφαρμόζουμε τον αλγόριθμο του Ευκλείδη:

gcd(a,b)=gcd(b,amodb)		πηλίκο	gcd	x	y
35	96	0	1	11	-4
96	35	2	1	-4	11
95	26	1	1	3	-4
26	9	2	1	-1	3
9	8	1	1	1	-1
8	1	8	1	0	1
1	0	-	1	1	0

Ο συντελεστής του 35 είναι το 11 (1η γραμμή) άρα d=11 και το μήνυμα είναι:

$M=5^{11} \mathrm{mod} 119$

Γράφουμε τη δυαδική αναπαράσταση του 11 και εφαρμόζουμε τον αλγόριθμο εύρεσης δύναμης:
$<11>_{10} \rightarrow <1011>_2$
M=1

$\underline{1}011$
$M \leftarrow M^2 \bmod 119 = 1$
$M \leftarrow M \cdot a \bmod 119 = 5$
$1\underline{0}11$
$M = 25$
$10\underline{1}1$
$M = 25^2 \bmod 119 = 30$
$M = 30 \cdot 5 \bmod n 119 = 31$
$101\underline{1}$
$M = 31^2 \bmod 119$
$M = 5 \cdot M \bmod 119$

Ερώτηση: Γιατί ελέγχουμε μόνο το 5^{11} και όχι το 5^{11+96k}; Γιατί $5^{11+96к} (\text{mod} 119) = =5^{11}(5^{96})^{k} (\text{mod} 119)$ και από το θεώρημα του Euler το $5^{96} \bmod 119 = 1$ άρα όλες οι υπόλοιπες τιμές απαλείφονται.

Θέμα (4 μονάδες)
Η Αλίκη και ο Μπόμπος μένουν σε μια χώρα με 50 πολιτείες, η Αλίκη στην πολιτεία a και ο Μπόμπος στην πολιτεία b. Η Αλίκη θέλει να μάθει αν ο Μπόμπος μένει στην ίδια πολιτεία με αυτή. Πώς μπορεί να το μάθει χωρίς ο Μπόμπος να πάρει καμία πληροφορία για την πολιτεία που μένει αυτή; Η Αλίκη και ο Μπόμπος επικοινωνούν με βάση το παρακάτω πρωτόκολλο:

Συμφωνούν σε ένα πρώτο p και το γεννήτορά του g.
<u>Αλίκη:</u>
διαλέγει τυχαία $x,y \in Z_p^*$
στέλνει στο Μπόμπο το μήνυμα $(A_0, A_1, A_2) = (g^x \bmod p, g^y \bmod p, g^{xy+a} \bmod p)$

<u>Μπόμπος:</u>
διαλέγει τυχαία $r,s \in Z_p^*$
στέλνει στην Αλίκη το μήνυμα $(B_1, B_2) = (A_1^r g^s \bmod p, (A_2 (g^b)^{-1})^r A_0^s \bmod p)$

Απάντηση:
$B_1 = (g^y \bmod p)^r g^s \bmod p = g^{yr} g^s \bmod p = g^{yrs} \bmod p$
$B_2 = [(g^{xy+a} \bmod p) g^{-b}]^r (g^x \bmod p)^s \bmod p = g^{r(xy+a)} g^{-br} g^{xs} \bmod p = g^{r(xy+a-b)+xs} \bmod p$
**Επειδή έχουμε μόνο προσθέσεις και πολλαπλασιασμούς, μπορούμε να αγνοήσουμε τα modp μέχρι το τέλος.

Αν a=b τότε
$B_2 = g^{rxy+xs} \bmod p = g^{x(ry+s)}$
Άρα αρκεί η Αλίκη να ελέγξει αν $B_1^x = B_2$. Αν ισχύει, τότε μένουν στην ίδια πολιτεία. Ο Μπόμπος δεν μπορεί να μάθει πού μένει η Αλίκη γιατί δεν γνωρίζει τα x,y,a και δεν μπορεί να τα βρει από πράξεις γιατί δεν μπορεί να λύσει το πρόβλημα του διακριτού λογαρίθμου. Με τον ίδιο τρόπο, η Αλίκη δεν γνωρίζει τα r,s,b, οπότε ούτε και αυτή μπορεί να βρει σε ποια πολιτεία μένει ο Μπόμπος.

Θέμα 2016 (1 μονάδα)
Να βρεθούν οι υποομάδες του Z_{15}^*

Απάντηση:
Βρίσκουμε πρώτα τα στοιχεία που ανήκουν στο Z_{15}, και ύστερα αφαιρούμε αυτά που δεν έχουν gcd(α,15)=1.
Z_{15}={~~0~~,1,2,~~3~~,4,~~5~~,~~6~~,7,8,~~9~~,~~10~~,11,~~12~~,13,14}

<1>={1} σταματάμε όταν βρούμε το ουδέτερο στοιχείο/όταν τα ψηφία αρχίσουν να επαναλαμβάνονται
<2>={2,4,8,1}
<4>={4,1}
…

Θέμα 2016
Πόσες λύσεις έχει η εξίσωση: $5x\equiv 7 \mod 5^{1000000}$

Απάντηση:
Η εξίσωση θα έχει λύση αν $\gcd(5,5^{1000000})|7=5|7$ που όμως δεν ισχύει, άρα δεν υπάρχει λύση για αυτή την εξίσωση.

Άσκηση
Έστω ότι χρησιμοποιείται το πρωτόκολλο Merkle-Hellman για την αποστολή ενός μηνύματος. Να βρεθεί το αρχικό μήνυμα M.
<u>Αλίκη:</u>
επιλέγει superincreasing ακολουθία a={1,2,4,8,16} και (w,n)=(11,37)
Η ακολουθία a μετατρέπεται στην ακολουθία b: (11,22,7,14,28) ταξινομείται και ανακοινώνεται δημόσια ως P_A={7,11,14,22,28}

<u>Μπόμπος:</u>
Παίρνει το κρυπτογραφημένο μήνυμα C=(32,64,47)

Απάντηση:
Ο Μπόμπος βλέπει ότι η P_A έχει 5 στοιχεία, οπότε χωρίζει το μήνυμα C σε block των 5 bit.

Το κομμάτι αυτό δεν ζητείται, ούτε και μπορούμε να το χρησιμοποιήσουμε ως λύση. Μπορούμε όμως να το χρησιμοποιήσουμε για να κάνουμε επαλήθευση.
$32=7b_4+11b_3+14b_2+22b_1+28b_0$ $M_1=11100$
$64=7b_4+11b_3+14b_2+22b_1+28b_0$ $M_2=00111$
$47=7b_4+11b_3+14b_2+22b_1+28b_0$ $M_3=01110$

$32\rightarrow 32(11)^{-1} \mod 37 \rightarrow$(επίλυση του $11x\equiv 1 \mod 37$ δίνει $x=27$)$\rightarrow 32\bullet 27 \mod 37=13$

Από την αρχική ακολουθία, το 13 είναι το άθροισμα των αριθμών 8,4,1 και κάνουμε αντιστοίχιση των δύο ακολουθιών για να βρούμε το αρχικό μήνυμα M_1. Ομοίως και με τα άλλα δύο μηνύματα.

Θέμα (4 μονάδες)
Έστω RSA με M=5. Η Αλίκη θέλει να στείλει ένα υπογεγραμμένο μήνυμα στο Μπόμπο. Το δημόσιο κλειδί της Αλίκης είναι $P_A=(n_A,e_A)=(65,29)$, το ιδιωτικό είναι $d_A=5$. Το δημόσιο κλειδί ου Μπόμπου είναι $P_B=(n_B,e_B)=(119,5)$, το ιδιωτικό είναι $d_B=77$. Δίνεται ότι 65=5•13 και 119=7•17. Να περιγράψετε αναλυτικά τη διαδικασία.

Άσκηση
Χρησιμοποιείται RSA με πολύ μεγάλο n ώστε να μην μπορεί να παραγοντοποιηθεί. Ο Μπόμπος κωδικοποιεί τα μηνύματά του ανά χαρακτήρα ως εξής: A=1,B=2,…,Z=25, =26. Είναι ασφαλές αυτό το πρωτόκολλο;

Απάντηση:
Το πρωτόκολλο δεν είναι ασφαλές γιατί μπορεί εύκολα να σπάσει με ανάλυση συχνοτήτων αν το μήνυμα είναι σε φυσική γλώσσα, χωρίς να χρειάζεται να βρεθεί το n